هيئة تنظيم الاتصالات TRA
TELECOMMUNICATIONS REGULATORY AUTHORITY

United Arab Emirates

UAE Information Assurance Regulation

Version 1.1

March 2020

Contents

Foreword 4

Chapter 1: Introduction 5
- 1.1 Background 6
- 1.2 Purpose of the UAE IA Regulation 8
- 1.3 Layout of the UAE IA Regulation 9

Chapter 2: UAE IA Regulation Overview 11
- 2.1 Scope 12
- 2.2 Related TRA Documents 12
- 2.3 Entity, Sector, and National Contexts 13
- 2.4 Information Assurance Lifecycle 14

Chapter 3: UAE IA Regulation Implementation 15
- 3.1 Overview 16
- 3.2 Risk-Based Approach 17
- 3.3 Applicability of Controls 20
- 3.4 Prioritization of Controls 21
- 3.5 Key Stakeholders Roles and Responsibilities 22
- 3.6 Key Success Factors 24

Chapter 4: Compliance with the UAE IA Regulation 25

Chapter 5: Security Controls 28
- 5.1 Control Structure 29
- 5.2 Description of families of controls 31
- 5.3 Management Controls 33
  - M1 Strategy and Planning 33
  - M2 Information Security Risk Management 49
  - M3 Awareness and Training 63
  - M4 Human Resources Security 69
  - M5 Compliance 77
  - M6 Performance Evaluation and Improvement 89
- 5.4 Technical Controls 94

T1 Asset Management 94

T2 Physical and Environmental Security 103

T3 Operations Management 114

T4 Communications 131

T5 Access Control 146

T6 Third-Party Security 167

T7 Information Systems Acquisition, Development and Maintenance 173

T8 Information Security Incident Management 195

T9 Information Systems Continuity Management 207

Annex A: Summary of Always Applicable Controls 215

Annex B: Summary of the Prioritized Controls 216

Annex C: Mapping of Controls against Leading Standards 224

Annex D: Mapping of Threats to Controls 235

Annex E: Sector and National Level Controls 238

Annex F: Terms and Definitions 240

Annex G: Bibliography 246

Foreword

The increased adoption of Information Technology (IT), electronic communications, and cyberspace - comprised of a global network of interdependent information technology infrastructures, telecommunications networks, and computer processing systems - has provided organizations in the UAE with a platform for delivering innovative services and stimulating economic development, as well as facilitating collaboration and communications among individuals. Our dependence on these technologies will continue to grow in the future, and therefore, the UAE Government is committed to the development of a secure national information and communications infrastructure for UAE organizations and individuals to realize the full potential of its benefits, in the face of an evolving set of related cyber threats.

As cyber threats such as hacktivism and cybercrime evolve, so must our efforts to defend against them in a coordinated and systematic manner. To align and direct national cyber security efforts, the UAE Government has multipliable initiatives to improve the national cyber security, and protect our national information and communications infrastructure. The UAE Information Assurance (IA) Regulation have been provide requirements for raising the minimum level of IA across all relevant entities in the UAE.

The adoption of these by UAE entities will sustain the benefits of a trusted digital environment for businesses and individuals across the nation. As cyber security is the shared responsibility of every organization and individual, collaboration and partnerships between the Government and private sector organizations are key to success. I am confident that our combined efforts will make great strides in achieving the UAE's national cyber security objectives and allow our nation's interests to thrive.

Chapter 1:
Introduction

1.1 Background

The adoption of Information Technology (IT) and electronic communication have greatly improved the efficiency and productivity of businesses and governments within the UAE, and facilitated collaboration of individuals within the nation and across the globe. Undoubtedly, IT and electronic communication have and will continue to play a pivotal role in the economic development of the UAE and the daily life of its citizens. Therefore, the UAE stands committed to the further development of its national IT and electronic communication infrastructure, as well as its cyberspace, to support economic development and provide an environment where the interests of its governments, businesses, and citizens can thrive.

The benefits of this technology adoption, however, come with a rapidly evolving set of cyber threats. These threats stem from a wide range of sources – including hacktivists, issue-motivated groups, and organized cybercrime syndicates – and represent national security concerns that can potentially disrupt critical national services and compromise critical information assets.

Mitigating cyber threats, and ensuring the development of a secure national information and communications infrastructure, and cyberspace, is a strategic priority for the UAE. To this end, TRATRA developed the UAE IA Regulation as a critical element of the National Information Assurance Framework (NIAF) to provide requirements for elevating the level of IA across all implementing entities in the UAE.

The development of the UAE IA Regulation is based on regional and global best practices including:

- ISO/IEC 27001:2005 "Information technology — Security techniques — Information security management systems — Requirements",
- ISO/IEC 27002:2005 "Information technology — Security techniques — Code of practice for Information security management",
- ISO/IEC 27005:2005 "Information technology — Security techniques —Information security risk management"
- ISO/IEC 27010:2012 "Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications"
- ISO/IEC 27032:2012 "Information technology — Security techniques — Guidelines for cybersecurity"
- NIST 800-53 Revision 4 "Security and Privacy Controls for Federal Information Systems and Organizations"

- Abu Dhabi Information Security Standards Version 1 and Version 2, developed by Abu Dhabi Systems and Information Centre (ADSIC).
- SANS 20 Critical Security Controls for Effective Cyber Defense Version 4.1

Moreover the development was guided by key principles including:

- Applicability of the common IA requirements across industries , and applicability of the sector-specific IA requirements across entities within each CIIP sector
- Support for the development of the entity, sector, and national-level views of cyber security, to address potential IA risks that emerge from the interconnectivity of entities and sectors
- Support the performance management and the evolution of the controls in these based on measuring and sharing effective performance indicators, as well as contributions from key stakeholders to support the ongoing development and refinement of these .

Compliance with these will raise the level of national IA and help the UAE progress towards a more resilient national information and communication infrastructure, and cyberspace. All UAE government entities and other entities identified as critical by TRA are obligated to implement these . However, TRA highly recommends all entities in the UAE to adopt these on a voluntary basis, as applicable, in order to participate in raising the nation minimum-security levels.

1.2 Purpose of the UAE IA Regulation

The purpose of the UAE IA Regulation is to provide requirements to raise the minimum level of protection of information assets and supporting systems across all implementing entities in the UAE, as outlined in Section 2.1.

In particular, the UAE IA Regulation provides:

- Description of how information assurance is achieved at the national, sector, and entity levels
- Enable a risk-based approach for the implementation of these
- Outline of the roles and responsibilities of key stakeholders for the planning, development, implementation, and ongoing monitoring and improvement of these
- Reference catalog of common information security controls to defend against common threats that exploit known cyber security vulnerabilities
- Realization for sectorial requirements through the provision of specialized controls to address sector-specific information assurance requirements
- Phased implementation approach to address the most common threats, facilitate the incremental adoption of these , and optimize the value realized through implementation
- Definition of compliance from the perspective of these and describe the approach that will be adopted by TRA to assess compliance
- Enabler for inter-entity and cross-sector communication to support information sharing and build national situational awareness

In summary, the implementation of these will serve to improve the IA protection level of the UAE critical information infrastructure. As such, this document serves as the national UAE IA Regulation that implementing entities have to demonstrate compliance with.

1.3 Layout of the UAE IA Regulation

This section provides an overview of the layout of the UAE IA Regulation to guide the readability of this document.

Overall, the UAE IA Regulation is composed of seven chapters:

- Chapter 1: **Introduction:** This chapter outlines TRA's rationale for developing the UAE IA Regulation and provides an overview of the document layout.

- Chapter 2: **UAE IA Regulation Overview:** This chapter outlines the scope of the document and describes the relationship of the UAE IA Regulation with other national cyber security program documents published by TRA (e.g. UAE CIIP Policy). This chapter also describes how information assurance requirements are addressed at the national, sector, and entity levels following a lifecycle approach to progress the adoption and evolution of information assurance in the UAE.

- Chapter 3: **UAE IA Regulation Implementation:** This chapter outlines the implementation guidance for entities applying the UAE IA Regulation. To help guide the implementation of these , this chapter also provides an overview of the risk-based approach for the identification of applicable controls to be implemented in order to address risks in a manner commensurate with their potential impact. Moreover, this chapter outlines the roles and responsibilities of key stakeholders to provide clarity on how to plan, develop, implement, monitor, improve, and report on the implementation of these . Lastly, this chapter concludes by outlining critical success factors for the effective implementation of these .

- Chapter 4: **Compliance with the UAE IA Regulation:** This chapter provides a definition of compliance with respect to the requirements of these , and outlines the approach that TRA will follow when evaluating compliance.

- **Chapter 5**: **Security Controls:** This chapter details the management and technical security controls, and describes the prioritization approach for implementing these controls, to guide the gradual and phased implementation of these .

- **Chapter 6**: **Annexes:** This chapter provides key reference tools to help stakeholders understand and utilize the security controls including: grouping of controls by priority, cross-referencing of controls to equivalent controls in other key IA Regulation, mapping of controls against common threats they help to manage, and listing the controls that contain sector and national level requirements. Lastly, this chapter enhances the clarity of the document by providing terms and definitions and a bibliography.

- **Chapter 7**: **Appendices:** The appendices are designed to augment the common information assurance requirements (applicable to all sectors) with sector-specific requirements for all critical sectors as outlined in the UAE CIIP Policy.

Chapter 2:

UAE IA Regulation Overview

2.1 Scope

The UAE IA Regulation provides management and technical information security controls (henceforth referred to as "security controls") for entities to establish, implement, maintain, and continuously improve information assurance.

TRA will designate the critical entities, as per the UAE CIIP Policy, mandated to implement the UAE IA Regulation and apply its requirements to the use, processing, storage, and transmission of information or data, and the systems and processes used for those purposes. This includes information in physical or electronic form that may be owned, leased, or otherwise in the possession, custody, or control of the entities.

2.2 Related Documents

The UAE IA Regulation are critical element of the National Cyber Security Strategy (NCSS). Given this, these rely on related and complementary policies issued under the NCSS. Table 1 below describes the relationships and dependencies between the UAE IA Regulation and some other NCSS policies:

Table 1: Overview of Documents Related to the UAE IA Regulation

Document	Relation to UAE IA Regulation
National Information Assurance Framework (NIAF)	• The NIAF document outlines key building blocks of the UAE information assurance capabilities and program, and specifies the entity, sector, and national information assurance interdependencies and requirements that need to be addressed as part of the UAE IA Regulation.
Critical Information Infrastructure Protection (CIIP) Policy	• The CIIP Policy establishes the list of sectors and outlines the process for the identification of critical entities where the UAE IA Regulation implementation is mandatory.
National Cyber Risk Management Framework (NCRMF)	• The National Cyber Risk Management Framework details the sector and national level risk management approach with regards to Critical National Services and their Critical Information Infrastructure, and provides guidelines on the implementation of risk assessment in this regard. As such, the UAE IA Regulation outline key elements to be included in an entity-level risk assessment, to support sector and national risk assessment activities.
National Cyber Information Sharing Policy	• The National Cyber Information Sharing policy outlines key requirements for inter-entity and inter-sector communication that serves as a key input to developing national situational awareness. The UAE IA Regulation address these requirements by embedding respective Information Sharing security controls that UAE entities will implement.

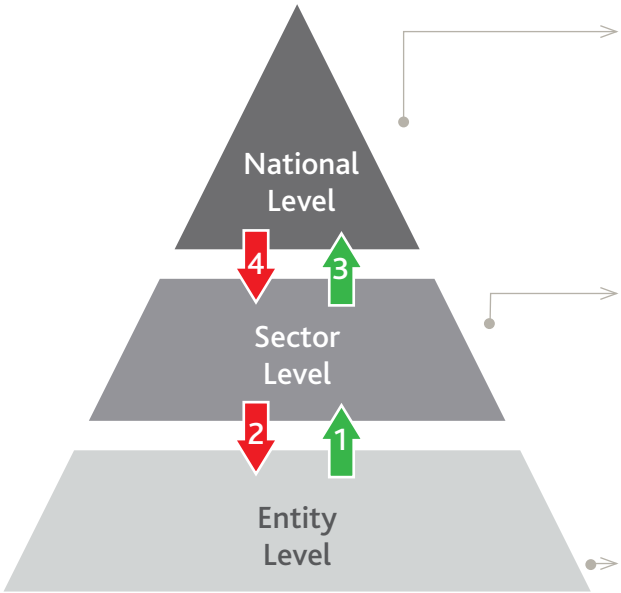
2.3 Entity, Sector, and National Contexts

The entity, sector, and national contexts refer to the integrated relationships and interactions among individual sector entities, sector regulators, and TRA to form sector and national level views on prevailing IA requirements, corresponding adequacy of IA capabilities, and on-going situational awareness.

While IA Regulation that exist today prescribe requirements for the entity level, they do not take into account the IA issues that emerge from the systemic interconnectivity of entities at the sector and national levels. This leads to two key shortcomings: first, continued exposure to security threats that no single entity is able to address individually (such as Advanced Persistent Threats), and second, an isolated approach to handling risks related to inter-sector dependencies, often leading to increased efforts, cost, and risk exposure of concerned sectors.

The UAE IA Regulation includes minimum IA requirements and capabilities for UAE entities to integrate into the Sector and National Contexts (refer to Figure 2).

Figure 2: National, Sector and Entity Context



4 TRA consolidates and analyzes the information reported by sector regulators to from a national and sector view on the state of the Regulation implementation , as well as the risks , and shares relevant threat and risk information with sector regulators to increase effectiveness of the incident management and risk assessment programs.

3 Sector regulators consolidate and analyze information reported by entities to from a sector view of risks and the state of the UAE IA Regulation implementation, and escalate key findings to TRA and other Cyber Security parties.

2 Sector regulators share relevant security threat, risk and incident information with entities to increase effectiveness of the incident management and risk assessment programs

1 Entities report key information to sector regulators, in particular relating to;

- State of the UAE IA Regulation implementation.
- Risk assessment outcomes
- Cyber security threats, risks and incidents

The development of the sector and national contexts relies on the consolidation and analysis of key entity level information, in particular relating to the state of the UAE IA Regulation implementation, risk assessment outcomes, as well as information relating to cyber security threats, risks and incidents. To enable the sector and national contexts, entities are required to submit UAE IA Regulation implementation progress and key cyber security information to sector regulators, who consolidate and analyze the information to form a sector view of risks and assess the state of these implementation. Similarly, sector regulators are required to submit the analyzed sector-level information to TRA and other cyber security parties, to form the national views on critical risks, situational awareness and state of these implementation across sectors.

Having formed the national view of risks and state of these implementation, TRA shares relevant risk and UAE IA Regulation implementation best practices with the sector regulators to enhance the effectiveness of these implementation, as well as the cyber incident management and the cyber risk management programs. Similarly, sector regulators share key risk and implementation related information with relevant entities to progress the implementation of these , and enhance the effectiveness of the incident management and risk management programs.
In summary, the UAE IA Regulation is designed to avoid the isolation created by a single-entity approach to IA, hence creating a stronger and more integrated approach for national information assurance.

2.4 Information Assurance Lifecycle

The UAE IA Regulation promotes a lifecycle approach for establishing, implementing, maintaining and continuously improving information assurance. This lifecycle approach ensures continual improvement of the UAE's information assurance capabilities based on well-defined activities:

a. Understanding an entity's and / or sector's information security requirements and the need to establish a policy and objectives for information security
b. Conducting risk assessments, identifying appropriate risk treatment actions, and selecting controls to manage the risks
c. Implementing and operating security controls to manage information security risks in the context of the entity's or sector's overall business risks
d. Monitoring and reviewing the performance and effectiveness of the information security processes and controls
e. Ensuring continual improvement based on objective measurements

The continuous improvement aspect of the IA lifecycle ensures that IA capabilities are continuously adapted and evolved in line with changing requirements. The application of the IA lifecycle is facilitated best when integrated in the planning and governance activities of an entity or sector.

Chapter 3:

UAE IA Regulation Implementation

3.1 Overview

The purpose of this chapter is to explain key concepts related to the implementation of the UAE IA Regulation such as the risk-based approach to information assurance and the applicability and prioritization of security controls. This chapter also highlights key stakeholder roles and responsibilities for the effective adoption and progression of the UAE IA Regulation, and it lists critical implementation success factors.

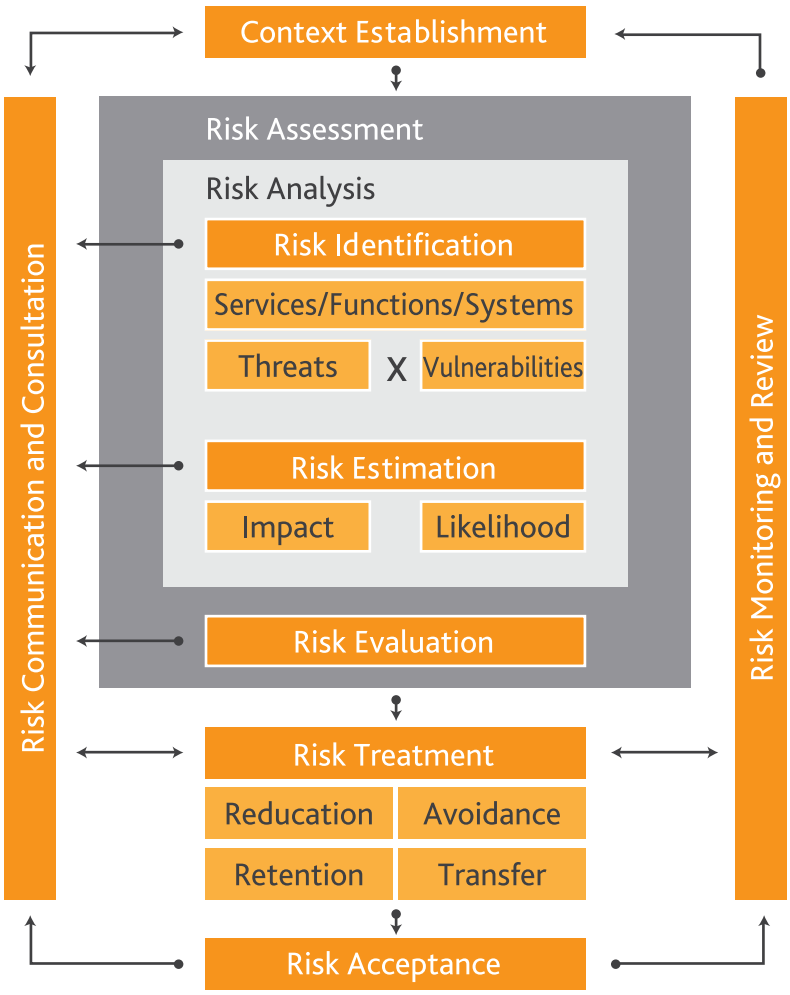
The implementation of this regulation is meant to complement any existing information assurance programs at implementing entities. This regulation represents the sole point of reference for compliance against its requirements, as measured by the criteria associated with each of its security controls.

3.2 Risk-Based Approach

In today's world, the cyber threat landscape is evolving rapidly at a pace where entities are challenged to keep up with the number and variety of threats. In the face of this growing threat landscape, entities need to adopt practical measures to defend their critical information and information infrastructure against their most critical vulnerabilities that could be exploited by threats. To this end, a risk-based approach provides entities with a pragmatic mean to identify their most critical vulnerabilities that could expose them to risks, and develop corresponding appropriate treatments.

Adopting a risk-based approach ensures that security controls are instituted in accordance with current risk assessments commensurate with the risk and magnitude of the impact that could result if critical information assets are compromised. The risk-based approach briefly outlined in these summarizes a systematic methodology for identifying, estimating, evaluating, and treating identified entity-level risks. It consists of eight key activities as illustrated in Figure 3.

Figure 3: The Risk-Based Approach Process



Performing a risk management is a key step towards the implementation of the UAE IA Regulation as it helps entities identify, prioritize, and measure the effectiveness of the security controls that are needed to treat identified entity-specific risks. Critical entities implementing these shall also refer to the National Cyber Risk Management Framework (NCRMF) which highlights the National Risk Management approach and process of Critical Information Infrastructure.

Activity 1: Establishing the Environment:

The risk assessment process should be initiated by establishing objectives, strategies, scope and parameters of the activities of the entity, or those parts of the entity where the risk management process is being applied. Further, criteria for assessing risks should be established in line with the entity's objectives, available resources, and the magnitude of impact that could result from the compromise of confidentiality, integrity and/or availability of information assets. Topics such as authenticity and non-repudiation could also be considered based on the entity context.

Activity 2: Risk Identification:

The entity should identify sources of risk, areas of impacts, events and their causes, and the potential consequences. The aim of this step is to generate a comprehensive list of risks based on the identified information security requirements. Because a risk that is not identified at this stage will not be included in further analysis, comprehensive identification is critical.

Activity 3: Risk Estimation:

Risk estimation involves consideration of the causes and sources of risk in the form of threats and vulnerabilities, their impacts in terms of consequences of a loss of confidentiality, integrity and/or availability of information, and the likelihood that the potential impacts will occur. The risk should also take into account the effectiveness and efficiency of existing controls in addressing the current level of risk.

Activity 4: Risk Evaluation:

Risk evaluation involves comparing the level of risk found during the risk estimation activity with risk criteria established at the beginning of the process as part of establishing the context (Activity 1). The objective is to determine which risks are outside acceptable parameters and therefore require treatment.

Activity 5: Risk Treatment:

For each of the risks identified in the risk assessment, a number of treatment options can be considered and applied either individually, or in combination, for treating the risk. There are

several options that are usually considered for treating risks; these options include:

- Risk Reduction – Reducing the risk by applying security controls. The selection of security controls should follow a risk-based approach by apply the first set of security controls that treat the highest risks identified during the Risk Evaluation (See 3.4 Prioritization of Controls).
- Risk Retention – Accepting the risk based on the entity's risk accepting criteria.
- Risk Avoidance – Avoiding the activity or condition causing the risk.
- Risk Transfer – Transferring the risk to another party.

Activity 6: Risk Acceptance:

The risk acceptance is the decision to accept residual risk by the management of the entity. The management based on the acceptance criteria should review and approve the treat plan and the residual risk.

Activity 7: Risk Monitoring and Review:

The results of the risk assessment and treatment process need to be monitored and reviewed for ongoing risk management, and to ensure their continued suitability. The monitoring and review of information security risks should be a planned part of the risk management process, and involve regular checking or surveillance as well as improvements when significant changes occur. The entity's monitoring and review processes should encompass all aspects of the risk management process, including the risk criteria, the identified assets, threats, risks, risk treatment options and security controls.

Activity 8: Risk Communication and Consultation:

Communication and consultation with key stakeholders should take place during all stages of the risk management process. Therefore, plans for communication and consultation should be developed at an early stage. These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Effective external and internal communication and consultation should take place to ensure that stakeholders and those accountable for implementing the risk management process understand the basis on which decisions are made, as well as the reasons why particular actions are required.

3.3 Applicability of Controls

The concept of Applicability relates to the identification of security controls for treating entity-specific risks as outlined in [Step 5] of the risk assessment process described above (section 3.2).

The security controls included in these are developed to treat a typical entity risk profile developed based on benchmark risk registers. While this common risk profile is widely applicable to implementing entities, TRA recognizes that entity risk profiles do differ based on their specific business and operational context. Given these differences, not all security controls provided in these might be applicable to all entities. Therefore, these require that the identification of the security controls be based on an entity risk assessment resulting in applicable security controls for the treatment of identified risks.
Prior to performing the risk assessment process, an entity should consider all security controls to be applicable. However, an individual entity may exclude some security controls on the basis of the risk assessment outcomes, provided that adequate justification is submitted to TRA.

Moreover, certain security controls included in these represent requirements for instituting foundational IA capabilities within an entity, and as such, are considered "Always Applicable". Given their foundational role, the "Always Applicable" security controls shall be implemented by each relevant entity regardless of its risk assessment outcomes (refer to Annex 1 for a summary of "Always Applicable" controls).

In summary, the concept of Applicability identifies the security controls that are mandatory for implementation based on the list of applicable controls resulting from the entity risk assessment process, above and beyond the "Always Applicable" controls. In the absence of an entity risk assessment, all the security controls detailed in these are deemed applicable and therefore mandatory for implementation.

3.4 Prioritization of Controls

The concept of Prioritization relates to grouping the UAE IA Regulation security controls in order of importance for realizing a minimum level of information assurance protection, and for enabling a phased and incremental implementation of these .

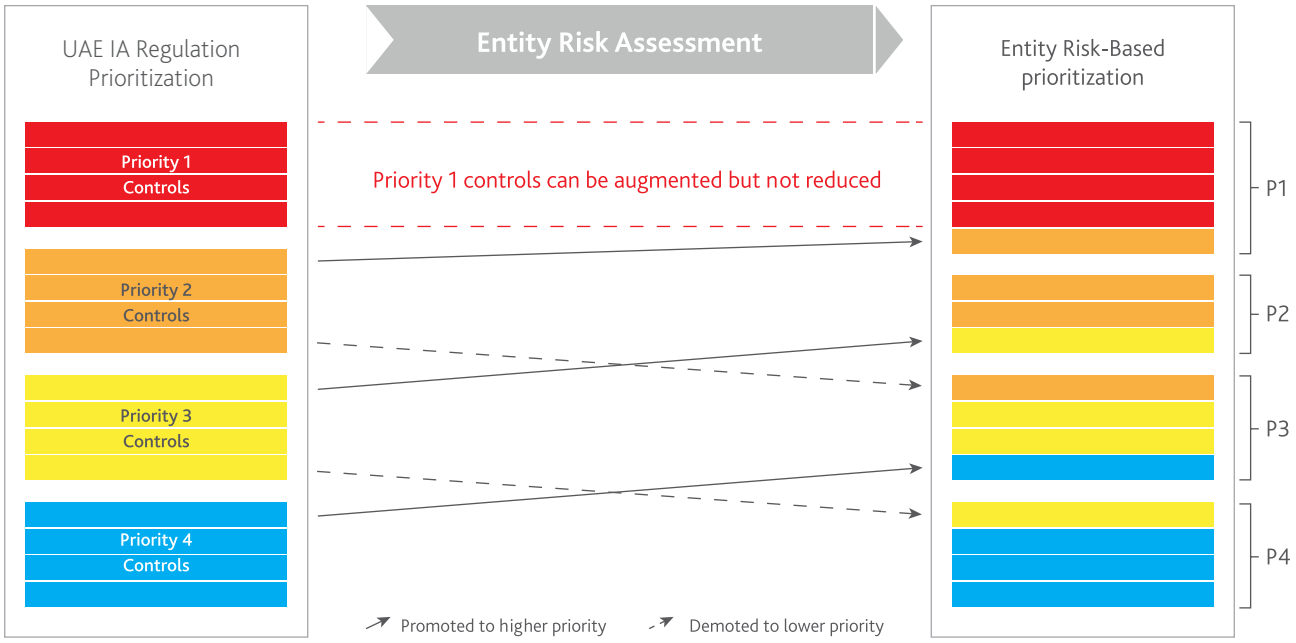
The prioritization approach of the UAE IA Regulation is based on the relative impact of security controls in helping implementing entities to:

- Mitigate common threats
- Build foundational IA capabilities

Based on these criteria, the security controls are grouped into four priority levels – P1, P2, P3, and P4 in this order of importance – and the outcome of the prioritization is included in Annex 2.

While all the applicable security controls across the four priority levels are mandatory for critical entities implementing these , they are required to begin implementing these with P1 security controls given their highest relative impact in protecting against critical threats and building foundational information assurance capabilities.
Critical entities implementing these may alter (promote or demote) the suggested priority of controls based on the outcomes of their risk assessment, with the exception of top priority controls

(P1), which if applicable, may be augmented but never reduced (refer to Figure 4).



3.5 Key Stakeholders Roles and Responsibilities

The successful implementation and progression of the UAE IA Regulation is a shared responsibility among key stakeholders. Therefore, planning, development, implementation, as well as monitoring and reporting responsibilities are assigned to key stakeholders, as described in Table 2 below:

#	Stakeholder	UAE IA Regulation Roles and Responsibilities
1	TRA	**Role** Provide strategic leadership and governance, coordinate stakeholder involvement for the development and implementation of the UAE IA Regulation, and ensure ongoing compliance monitoring, and information sharing **Responsibilities** **IA Regulation Planning and Development** • Information Assurance Strategy Development – Provide strategic priorities for the development of the common and sector-specific requirements of the UAE IA Regulation • Security Requirements Development – Establish the UAE IA Regulation security requirements in collaboration with key stakeholders including sector regulators, critical entities and cyber security experts • UAE IA Regulation Issuance – Approve and publish the UAE IA Regulation as developed in collaboration with the key stakeholders **IA Regulation Implementation** • TRA is responsible for facilitating the implementation of the UAE IA Regulation, but does not have direct responsibilities in the implementation of these within implementing entities **IA Regulation Monitoring and Reporting** • Compliance Monitoring – Review entity compliance self-assessment reports (as received from sector regulators), and recommend escalation for Compliance Audits or Testing where appropriate. • Compliance Audit – Where appropriate, perform or commission compliance audits for validating entity self-assessment reports, and escalate further, if needed • Compliance Testing – Where appropriate, perform or commission tests on relevant entities for ensuring that IA measures are in place, as well as their effectiveness • Cyber Security Performance Reporting – Compile progress reports of the UAE IA Regulation implementation across sectors and entities to steer the implementation efforts of these

#	Stakeholder	UAE IA Regulation Roles and Responsibilities
		Role
2	Sector Regulators	Actively contribute to the development of the UAE IA Regulation in collaboration with TRA, developing sector specific IA requirements/controls, and ensure UAE IA Regulation compliance reporting as well as information sharing Responsibilities **IA Regulation Planning and Development** • UAE IA Regulation Development – Provide input in the development of the UAE IA Regulation security requirements in collaboration with TRA • Sector-Specific Requirements Development – Augment UAE IA Regulation with sector-specific requirements pertinent to each critical sector **IA Regulation Implementation** • Sector Regulators are responsible for facilitating the implementation of the UAE IA Regulation, but do not have direct responsibilities in the implementation of these within relevant entities **IA Regulation Monitoring and Reporting** • Sector Compliance Reporting – Consolidate critical entity compliance reports into a sector status update, and submit report to TRA to form a sector and potentially national view on the IA Regulation implementation progress
		Role
3	Implementing Entities	Implement the UAE IA Regulation, and report on implementation progress and compliance, as well as share insights on security controls effectiveness Responsibilities **IA Regulation Planning and Development** • IA Regulation Development – Provide input in the development the UAE IA Regulation security requirements in collaboration with TRA through the IATFs • Entity Implementation Plan Development – Develop an implementation plan for the adopting/applying the UAE IA Regulation **IA Regulation Implementation** • Risk Assessment – Conduct risk assessment exercise to identify most critical vulnerabilities/threats and develop corresponding appropriate treatments • IA Regulation Implementation – Implement applicable controls from the UAE IA Regulation **IA Regulation Monitoring and Reporting** • Compliance Reporting – Periodically update the relevant regulator (or TRA in the absence of a "Sector-Regulator") on the progress of UAE IA Regulation implementation, and facilitate the audit and testing process whenever requested by the TRA

3.6 Key Success Factors

The implementation of the UAE IA Regulation and related security controls should be guided by the following key success factors:

a. Provide appropriate awareness, training, and education within the entity, and communicate information assurance objectives to all managers, employees, and other organizational stakeholders (including partners, third-party vendors, etc.)
b. Establish a thorough understanding of the information assurance requirements, and in particular, the risk-based approach to identify applicable security controls and their respective implementation priorities
c. Adopt a tailored approach and framework to establish, implement, maintain, and continuously improve information security in a manner that is consistent with the entity's culture
d. Understand the means by which compliance with the UAE IA Regulation will be measured and enforced
e. Implement a measurement system to track compliance, evaluate performance in information assurance management, and provide feedback and suggestions for the improvement and refinement of the UAE IA Regulation
f. Escalate critical cyber security information to sector regulators (or equivalents) to enable the development of sector and national level view of risks
g. Participate, and contribute in sharing information assurance best practices and lessons learned with sector regulators and other implementing entities
h. Ensure visible support and commitment from all levels of management
i. Provision adequate funding for all information assurance activities

Chapter 4:

Compliance with the UAE IA Regulation

The purpose of this chapter is to provide a definition of compliance with respect to the requirements of these and to outline the measurement criteria and approach that TRA will follow when evaluating compliance.

Within the context of this Regulation, compliance refers to the comparison between the requirements outlined in this Regulation and the actual state of implementation of these requirements within an entity. This can be measured on an individual control basis, as well as the degree of compliance of an entity overall with the complete set of requirements. Increasing the level of compliance with the security controls provided in this Regulation is the key to ensuring immediate and long lasting improvements of information assurance within the UAE and the overall success of the UAE's Information Assurance program. To this end, TRA will ensure that an effective compliance monitoring scheme is in place which provides TRA with the visibility of the current status of compliance with this Regulation and the activities needed for improving the overall security of the UAE's cyberspace. The compliance monitoring scheme is outlined in the UAE NIAF Governance and is based on the following four elements:

Controls:

All security controls specified in the UAE IA Regulation need to be considered by each entity, and any entity wishing to claim compliance with these shall implement these controls based on the following requirements:

- Controls that are "Always Applicable" – these security controls are essential and shall be implemented by any entity wishing to claim compliance with the UAE IA Regulation. Omission of any of these controls is not acceptable and constitutes non-conformity.
- Controls that are applicable based on the risk assessment – the entity shall determine which of the security controls provided in the UAE IA Regulation are applicable in its particular situation based on the results of the risk assessment. Any exclusion of these controls needs to be justified and evidence needs to be provided such that the associated risks have been accepted by accountable persons or authorizing entities.

The overall set of security controls that are "Always Applicable" and those security controls that have been determined as being applicable based on the risk assessment are "mandatory" for the entity to implement, and will be the basis of the compliance monitoring scheme.

Sub-Controls:

For each of the security controls, a set of sub-controls are specified. These sub-controls specify mandatory implementation requirements. Also, it is expected that each entity claiming compliance shall implement the selected security controls by complying with the sub-controls during the implementation process as described below.

The entity shall implement all of the sub-controls of the "Always Applicable" security controls. Omission of any of these sub-controls is not acceptable and constitutes non-conformity to the UAE IA Regulation.

The entity can decide to not implement a sub-control of a security control identified by the risk assessment, if this action is appropriately justified (e.g. following the risk assessment or due to decisions or circumstances in the entity), or to implement the sub-controls in a different way. Any deviation from the sub-controls needs to be justified and evidence needs to be provided such that the associated risks have been accepted by accountable persons or authorizing entities.

Performance Indicators:

Performance indicators are intended to provide entities implementing the UAE IA Regulation with some basic guidelines to measure the quality and effectiveness of its compliance with the control sub-families and controls of this Regulation. Entities implementing this Regulation can deviate from these performance indicators, but are required to provide a reason for this deviation and to specify the new performance indicators when doing so.

For compliance with this Regulation, entities need to use performance indicators to measure the quality and effectiveness of the implemented security controls.

Automation, Threat/Vulnerability Description for Sub-Families of Controls, and Implementation Guidance for Controls:

The information on possible automation and the implementation guidance for security controls are provided for information purposes only and can be implemented as the entity prefers, without any further explanation or justification. Descriptions of typical threats and vulnerabilities are also provided for information purposes.

In summary, TRA places a high level of importance on understanding and improving the level of compliance with this Regulation as one of the core elements of increasing the level of success of the UAE's information assurance program. At the same time, TRA understands that individual entities face specific circumstances that require a certain level of flexibility to manage properly. As such, this Regulation aims to strike an appropriate balance of mandatory requirements versus suggested security controls. This is based on the risk-based approach that each entity shall develop internally in order to make appropriate and justified decisions. Moreover, all implementing entities are welcomed and encouraged to share their experience in regard to the implementation of the security controls.

Chapter 5:
Security Controls

5.1 Control Structure

The hierarchy of control families, control sub-families and individual controls are structured as follows:

Control Family Number

Control Family Number	Control Family Name
Objective	High level objective of the control family
Performance Indicator	Metrics that measure the effectiveness of the control family

Sub-Family Structure

Control Sub-Family Number	Control Sub-Family Name
Objective	High level objective of the control sub-family
Performance Indicator	Metrics that measure the effectiveness of the control sub-family
Automation Guidance	Description of procedures and / or tools to automate the implementation of the control sub-family
Relevant Threats and Vulnerabilities	The most prevalent and damaging attack types against which the control sub-family ensures protection

Control Structure

Control Number	Control Name	Control Name	P1	P2	P3	P4
		Applicability	Identifies controls that are always applicable and controls that are applicable unless otherwise justified by the entity's risk assessment process			
Control	Control statement (e.g. The allocation and use of privileges should be restricted and controlled)					
Sub-Control	Sub-control statements that ensure optimal implementation of the control					
Implementation Guidance (for information purpose only)						
Additional information on how to implement individual controls, and what it requires Most of this information is derived from a variety of sources, including:						

- ISO/IEC 27001:2005 "Information technology — Security techniques — Information security management systems — Requirements"
- ISO/IEC 27002:2005 "Information technology — Security techniques — Code of practice for Information security management"
- ISO/IEC 27005:2005 "Information technology — Security techniques —Information security risk management"
- ISO/IEC 27010:2012 "Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications"
- ISO/IEC 27032:2012 "Information technology — Security techniques — Guidelines for cybersecurity"
- NIST Special Publication 800-53 Revision 4 "Security and Privacy Controls for Federal Information Systems and Organizations"
- Abu Dhabi Information Security Standards Version 1 and Version 2, developed by Abu Dhabi Systems and Information Centre (ADSIC)
- SANS 20 Critical Security Controls for Effective Cyber Defense Version 4.1

5.2 Description of families of controls

The security controls are structured under six management control families (addressing management requirements) described in Table 3 and nine technical control families (addressing technical requirements) described in Table 4.

Table 3: Description of Management Control Families

Management Control Families	Description
Strategy and Planning	An information security strategy shall be defined and operating model developed to adhere to the strategy. In addition, information security plans shall be developed for each major service to identify and mitigate the risks corresponding to each service
Information Security Risk Management	An information security risk management process shall be implemented to conduct risk assessments, statements of applicability, security testing and evaluations of information security controls on applicable services An awareness and training program shall be implemented to inform entities of risks associated with their activities and to ensure that entities are adequately trained to carry out their assigned information security responsibilities
Awareness and Training Human Resources Security	Human resources security requirements and security responsibilities shall be addressed prior employment, during employment, and after termination or change of employment
Compliance	Entities shall comply with legal requirements, security policies and technical standards
Performance Evaluation and Improvement	Entities shall ensure that information security performance is measured, analyzed and evaluated.

Table 4: Description of Technical Control Families

Technical Control Families	Description
Asset Management	Assets shall be managed and information shall be classified and labeled to ensure that assets including information receives an appropriate level of information security.
Physical and Environmental Security	Physical and environmental security measures shall be implemented to ensure critical or sensitive information systems are physically protected from unauthorized access, damage and interference and equipment is protected from physical and environmental threats.
Operations Management	Operational procedures and responsibilities shall be developed, to ensure an adequate level of information security. In addition, backup, media handling, e-services security and monitoring shall be addressed to ensure protection against malicious code and spyware.
Communications	Network security and information sharing shall be addressed to ensure protection of information in transit.
Access Control	Access control processes shall be developed to control access to information, to manage user access, control access to both internal and external network services, control access to operating systems, control access to applications and to apply appropriate protection when using mobile computing and teleworking services.
Third Party Security	Third party security shall be managed to ensure third parties implement and maintain the appropriate level of information security and service delivery, and information stored, processed, and retrieved, including via cloud services, is secure.
Information Systems Acquisition, Development and Maintenance	An information systems acquisition, development and maintenance process shall be implemented to prevent unauthorized modification or misuse of information in applications, to ensure that a cryptographic control policy is in place, to maintain security in development and support processes and to manage technical vulnerabilities.
Information Security Incident Management	Information security events and weaknesses shall be reported and evidence of security incidents shall be collected and analyzed to ensure that information security events and weaknesses are properly communicated and security incidents adequately managed.
Information Security Continuity Management	A business continuity management process shall be implemented to counteract interruptions to business activities and to protect critical business processes from failures of information systems.

5.3 Management Controls

M1 Strategy and Planning

M1	Strategy and Planning
Objective	To provide an adequate organizational environment, leadership and support for information security.
Performance Indicator	Percentage of incidents that are related to non-technical information security problems over one month

M1.1	Entity Context and Leadership
Objective	To establish leadership and a management framework to initiate and control the implementation of information security within the entity.
Performance Indicator	Measurement of the knowledge regarding information security roles and responsibilities, role of top management, etc., e.g. by using a test.
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Insufficient resources • Non-compliance with information security controls • Incompetent information security personnel • Incomplete or not up to date documentation

M1.1.1	Understanding the Entity and its Context	Priority	P1
		Applicability	Always applicable
Control	The entity shall determine external and internal factors that affect its ability to achieve the intended success of information security arrangements.		
Sub-Control	The entity shall determine: 1) interested parties that are relevant to its information security 2) the requirements of these interested parties 3) factors related to its sector or national context 4) its internal capabilities 5) its organizational structure		

Before starting the design and implementation of information security within an entity, it is important to evaluate and understand both the external and internal context of this entity, since these can significantly influence the design of information security solutions. For the external factors, this activity should include topics such as:

a. the industry sector, legal, regulatory, financial, technological, economic, political, natural and competitive environment, whether international, national, regional or local
b. key drivers and trends having impact on the information security objectives of the entity

c. relationships with, and dependencies of, external stakeholders

The evaluation of internal factors should address topics such as:
a. governance, organizational structure, roles and accountabilities;
b. capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies)
c. information systems, information flows and decision making processes
d. relationships with, and perceptions of, internal stakeholders
e. the form and extent of contractual relationships

M1.1.2	Leadership and Management Commitment	Priority	P1
		Applicability	Always applicable
Control	The entity's top management shall demonstrate leadership and commitment to information security.		
Sub-Control	Top management commitment shall: 1) ensure the information security policy and the information security objectives are established and are compatible with the strategic direction of the entity 2) ensure the integration of the information security requirements into the entity's processes 3) ensure that the resources needed for information security are available 4) communicate the importance of the effectiveness of information security management 5) direct and support persons to contribute to the effectiveness of information security and conforming to the requirements of these 6) promote continual improvement 7) support other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility 8) give direction to and participating in reviews of information security, including risks, controls and effectiveness, on a high level		

Implementation Guidance (for information purpose only)

Top management commitment and its visible demonstration is one important contributor to the overall success of information security within an entity. This does not mean that top management is carrying out the actions listed above themselves, but they need to ensure that the actions do take place, and that they are concluded successfully.

One important part in these responsibilities is the assignment of appropriate resources, without which information security cannot succeed (see also M1.4.1 below). Another important aspect is the connection between business goals and requirements and information security. Ideally, this is a balance between these items, and it should never be the case that information security hinders the business. It should, of course, also not be the case that an entity takes any unjustified risks and neglects security. The final decision what takes preference has to be taken by top management.

Management should identify the needs for internal or external specialist information security advice, and review and coordinate results of the advice throughout the entity.

M1.1.3	Roles and Responsibilities for Information Security	Priority	P1
		Applicability	Always applicable
Control	The entity shall ensure that the responsibilities and authorities of roles for information security are assigned and communicated.		
Sub-Control	Top management shall assign the responsibility and the authority for: 1) ensuring that the information security implemented in the entity conforms to the requirements of the UAE IA Regulation 2) reporting on the performance of information security to top management Top management shall ensure that 3) an Information Security Manager is appointed to take overall responsibility for the establishment, implementation, maintenance and continual improvement of information security 4) an Information Security Committee is established that oversees and governs the establishment, implementation, maintenance and continual improvement of information security in the entity, and that integrates information security in the entity		

Implementation Guidance (for information purpose only)

The roles of the "Information Security Manager" and the "Information Security Committee" are important contributors to successful information security, and have therefore been defined as sub-controls. When implementing these sub-controls, please keep in mind that it is important to address these roles, but the name and way of implementation of these roles can be chosen by the entity.
The Information Security Committee should have a leading role for information security in the entity and should be responsible for handling the important information security issues. The members of the Information Security Committee should have a sufficient understanding of information security for directing, monitoring, and completing the necessary tasks. Typical tasks of an Information Security Committee could be:

a. defining and establishing roles and responsibilities for information security
b. monitor the adequacy of resources to maintain and improve information security in the entity and recommend to management the acquiring of additional resources where necessary
c. providing input into the development, approval and implementation of information security policies and procedures
d. discussing practical issues regarding the implementation of information security policies and procedures and providing feedback from their respective parts of the entity
e. ensure that the status of information security risks is up to date and approve the updated risk assessment
f. recommending changes to policies and procedures based on security incidents and changes in risks
g. deciding the criteria for accepting information security risks and the acceptable levels of risk
h. identifying significant trends and changes to information security risks
i. review the results of performance measurement activities
j. reviewing audit reports and initiating appropriate corrective actions

The Information Security Manager should be the focal point for information security within the entity and should be responsible to direct the information security team (if present) and to provide valuable input into the Information Security Committee.

Additional responsibilities, such as technical security managers or asset owners can also be identified, as needed to implement information security in the entity. If necessary, roles and responsibilities should also be defined from contractors and third party users, and it should be ensured that all roles and responsibilities are reviewed periodically and kept up to date.

It is of particular importance that all people are aware of their responsibilities for information security and that everybody is aware of their duty to report information security incidents and events.

M1.2	Information Security Policy
Objective	To provide a framework and management direction and support for information security in the entity, in accordance with business requirements and relevant laws and .
Performance Indicator	Percentage of incidents that have been identified within the last month, which are related to non-compliances with any of the existing information security policies and procedures.
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Breaches of information security • Unawareness of policies and procedures • Non-compliance with information security controls

M1.2.1	Information Security Policy	Priority	P1
		Applicability	Always applicable
Control	The entity's top management shall establish a policy for information security in the entity.		
Sub-Control	The information security policy shall: 1) be appropriate to the purpose of the entity 2) provide the framework for setting information security objectives and/or include information security objectives (refer to M2.3.5) 3) include a commitment to satisfy all applicable information security requirements 4) include a commitment to continual improvement of the information security management system 5) be documented 6) be maintained, reviewed and updated at planned intervals or if significant changes occur		

Implementation Guidance (for information purpose only)

When developing the information security policy as well as the supporting policies (Control M1.2.2), take into account relevant TRA's issuances and guidance in this regard.

The following information should be considered for inclusion in the information security policy:

a. Statement related to management commitment and support of the goals and principles of information security in line with the business strategy and objectives
b. Description of the entity's approach to managing information security
c. Definition of information security in terms of confidentiality, integrity and availability
d. Reference to the entity risk management policy and the entity's approach to information security risk management
e. Reference to other risk management activities taking place in the entity, and how the information security risk management relates to that
f. Importance of compliance with the information security policy, and all supporting information security policies and procedures, and consequences of violations
g. Requirements of particular importance to the entity, e.g.:
   - compliance with legislative, regulatory, sector and contractual requirements
   - security education, training, and awareness requirements
   - business continuity management
h. Definition of general and specific responsibilities for information security, including reporting information security incidents
i. References to supporting information security policies and procedures

This information security policy should be communicated throughout the entity in a form that is relevant, accessible and understandable to the intended reader.

The information security policy should be written in a way that it can also be communicated to outsiders, e.g. outsourcing partners or contractors.

M1.2.2	Supporting Policies for Information Security	Priority	P2
		Applicability	Always applicable
Control	The entity shall establish and communicate a set of supporting policies for information security		
Sub-Control	The set of supporting information security polices shall: 1) be defined, approved, published and communicated to employees and relevant external parties 2) address all aspects of information security that are included in this Regulation, based on the risk assessment 3) address sector-specific and standards 4) be suitable to the entity and shall have a clearly identified audience 5) reflect the implementation the entity has chosen and shall not include any statements the entity does not comply with 6) include commitment of the Top Management 7) be documented 8) be maintained, reviewed and updated at planned intervals or if significant changes occur		

Implementation Guidance (for information purpose only)

The information security policy (refer to M1.2.1) should be supported by a set of supporting policies that address specific information security topics. Examples of topics to be addressed are:

a. logical access control
b. information classification and handling
c. physical security
d. end user oriented topics such as:

   - acceptable use of assets
   - clear desk and clear screen
   - email and Internet
   - mobile devices
   - restrictions on software installations and use
   - media security

e. backup & recovery
f. information exchange/sharing and transfer
g. malware protection
h. patch management
i. cryptographic controls
j. supplier relationships

These policies should be communicated to users in a form that is relevant, accessible and understandable to the intended reader, and sufficient training and awareness should be put in place to ensure that all users of these policies have understood and are aware of their content. It is also recommended to include the acceptance of compliance with all applicable policies and procedures in the induction process.

M1.3	Organization of Information Security
Objective	To establish a management framework to initiate and control the implementation of information security within the entity
Performance Indicator	Percentage of Top Management/Business Owners involved in the Information Security program. Measure the percentage of strategic information security decisions submitted and reviewed by the top management.
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Breaches of information security • Unawareness of policies and procedures • Non-compliance with information security controls • Insufficient resources

M1.3.1	Authorization Process for Information Systems	Priority	P2
		Applicability	Always applicable
Control	The entity shall establish a management authorization process for new information systems.		
Sub-Control	The entity shall: 1) define and implement a management authorization process for new information systems 2) regulate the use of personal information systems for processing business information		
Implementation Guidance (for information purpose only)			

The following guidelines should be considered for the authorization process:

a. new facilities should have appropriate user management authorization, authorizing their purpose and use. Authorization should also be obtained from the manager responsible for maintaining the local information system security environment to ensure that all relevant security policies and requirements are met;
b. where necessary, hardware and software should be checked to ensure that they are compatible with other system components;
c. the use of personal or privately owned information systems, e.g. laptops, home-computers or hand-held devices, for processing business information, may introduce new vulnerabilities and necessary controls should be identified and implemented.

M1.3.2	Confidentiality Agreements	Priority	P2
		Applicability	Always applicable
Control	The entity shall establish requirements for confidentiality or non-disclosure agreements reflecting the entity's needs for the protection of information.		
Sub-Control	The entity shall: 1) define a Non-Disclosure Agreement (NDA) template to be used to legally protect confidential information and ownership of information 2) have an information classification process in place to identify which information is subject to the terms of the NDA 3) Keep a track record of all signed NDAs and perform a periodical review		

Implementation Guidance (for information purpose only)

Confidentiality or non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. To identify requirements for confidentiality or non-disclosure agreements, the following elements should be considered:

a. a definition of the information to be protected (e.g. confidential information);
b. expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely;
c. required actions when an agreement is terminated;
d. responsibilities and actions of signatories to avoid unauthorized information disclosure (such as 'need to know');
e. ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information;
f. the permitted use of confidential information, and rights of the signatory to use information;
g. the right to audit and monitor activities that involve confidential information;
h. process for notification and reporting of unauthorized disclosure or confidential information breaches;
i. terms for information to be returned or destroyed at agreement cessation; and
j. expected actions to be taken in case of a breach of this agreement.

Based on an entity's security requirements, other elements may be needed in a confidentiality or non-disclosure agreement.

Confidentiality and non-disclosure agreements should comply with all applicable laws and for the jurisdiction to which it applies.

Requirements for confidentiality and non-disclosure agreements should be reviewed periodically and when changes occur that influence these requirements.

M1.3.3	Contact with Authorities	Priority / Applicability	P4 — Based on risk assessment
Control	The entity shall maintain appropriate contacts with relevant authorities.		
Sub-Control	The entity shall: 1) identify all relevant national authorities, including sector specific regulators 2) identify a Point of Contact in the Entity and communicate his/her name to the identified authorities, if required or allowed 3) establish a policy to determine when and how to engage relevant authorities		

Implementation Guidance (for information purpose only)

Entities should have procedures in place that specify when and by whom authorities (e.g. law enforcement, fire department, supervisory authorities) should be contacted, and how identified information security incidents should be reported in a timely manner if it is suspected that laws may have been broken. (Refer to Information Security Events and Weaknesses Reporting T8.3).

Entities under attack from the Internet may need external third paries (e.g. an Internet service provider or telecommunications operator) to take action against the attack source. Contact with authorities also could include external working groups.

M1.3.4	Contact with Special Interest Groups	Priority / Applicability	P4 — Based on risk assessment
Control	The entity shall maintain, as far as possible, appropriate contacts with relevant special interest groups.		
Sub-Control	The entity shall: 1) identify all relevant national and international interest groups or working groups or other specialist security forums and professional associations 2) allocate the right resources in order to properly support the group 3) define what participating employees are allowed to share 4) allow sharing and circulation of information inside the entity, as permitted by interest group rules		

Implementation Guidance (for information purpose only)

Membership in special interest groups or forums should be considered as a means to:

a. improve knowledge about best practices and staying up to date with relevant security information;
b. ensure the understanding of the information security environment is current and complete;
c. receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities;
d. gain access to specialist information security advice;
e. share and exchange information about new technologies, products, threats, or vulnerabilities;
f. provide suitable liaison points when dealing with information security incidents.

M1.3.5	Identification of Risks Related to External Parties	Priority	P1
		Applicability	Based on risk assessment
Control	The entity shall identify and properly manage the risks related to its information and information systems from business processes involving external parties		
Sub-Control	The entity shall: 1) identify risks to its information and information systems and implement the appropriate controls before granting access to any external party 2) define an external party access policy 3) identify and adopt proper controls to limit physical and logical access to information assets and entity information systems 4) monitor external party access to entity information and entity information systems		

Implementation Guidance (for information purpose only)

Where there is a need to allow an external party access to the information systems or information of an entity, a risk assessment should be carried out to identify any requirements for specific controls. The identification of risks related to external party access should take into account the following issues:

a. the information systems an external party is required to access;
b. the type of access the external party will have to the information and information systems, e.g.:
   1- physical access, e.g. to offices, computer rooms, filing cabinets;
   2- logical access, e.g. to an entity's databases, information systems;
   3- network connectivity between the entity's and the external party's network(s), e.g. permanent connection,remoteaccess;
   4- whether the access is taking place on-site or off-site;
c. the value and sensitivity of the information involved, and its criticality for business operations;
d. the controls necessary to protect information that is not intended to be accessible by external parties;
e. the external party personnel involved in handling the entity's information;
f. how the entity or personnel authorized to have access can be identified, the authorization verified, and how often this needs to be reconfirmed;
g. the different means and controls employed by the external party when storing, processing, communicating, sharing and exchanging information;
h. the impact of access not being available to the external party when required, and the external party entering or receiving inaccurate or misleading information;
i. practices and procedures to deal with information security incidents and potential damages, and the terms and conditions for the continuation of external party access in the case of an information security incident;
j. legal and regulatory requirements and other contractual obligations relevant to the external party that should be taken into account;
k. how the interests of any other stakeholders may be affected by the arrangements.

Access by external parties to the entity's information should not be provided until the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. Generally, all security requirements resulting from work with external parties or internal controls should be reflected by the agreement with

the external party.

It should be ensured that the external party is aware of their obligations, and accepts the responsibilities and liabilities involved in accessing, processing, communicating, or managing the entity's information and information systems.

M1.3.6	Addressing Security When Dealing With Customers	Priority / Applicability	P2 / Based on risk assessment
Control	The entity shall address all identified security requirements before giving customers access to the entity's information or assets.		
Sub-Control	The entity shall: 1) make sure that any customer accessing entity information and information systems are compliant with the entity's information security policy and security requirements 2) monitor any customer access and verify compliance to agreed access control policy		

Implementation Guidance (for information purpose only)

The following terms should be considered to address security prior to giving customers access to any of the entity's assets (depending on the type and extent of access given, not all of them might apply):

a. asset protection, including:
   1- procedures to protect the entity's assets, including information and software, and management of known vulnerabilities;
   2- procedures to determine whether any compromise of the assets, e.g. loss or modification of data, has occurred;
   3- integrity;
   4- restrictions on copying and disclosing information;
b. description of the product or service to be provided;
c. the different reasons, requirements, and benefits for customer access;
d. access control policy, covering:
   1- permitted access methods, and the control and use of unique identifiers such as user IDs and passwords;
   2- an authorization process for user access and privileges;
   3- a statement that all access that is not explicitly authorized is forbidden;
   4- a process for revoking access rights or interrupting the connection between systems;
e. arrangements for reporting, notification, and investigation of information inaccuracies (e.g. of personal details), information security incidents and security breaches;
f. a description of each service to be made available;
g. the target level of service and unacceptable levels of service;
h. the right to monitor, and revoke, any activity related to the entity's assets;
i. the respective liabilities of the entity and the customer;
j. responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, e.g. data protection legislation, especially taking into account different national legal systems if the agreement involves co-operation with customers in other countries;
k. intellectual property rights (IPRs) and copyright assignment and protection of any collaborative work.

M1.3.7	Addressing Security in Third Party Agreements	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall have agreements that cover all relevant security requirements with third parties to handle the entity's information assets		
Sub-Control	The entity shall: 1) verify that any contract or agreement with third parties addresses all aspects of the entity's information security policy regarding accessing, processing, communicating or managing the entity's information or information systems, or adding products or services to information systems 2) make sure that proper controls are introduced in the contract in order to verify compliance with the agreed security objectives (refer to T6) 3) perform audit of third parties services and infrastructures to verify compliance with agreed security objectives		

Implementation Guidance (for information purpose only)

The agreement should ensure that there is no misunderstanding between the entity and the third party. Entities should satisfy themselves as to the indemnity of the third party.

The following terms should be considered for inclusion in the agreement in order to satisfy the identified security requirements:

a. the information security policy;
b. controls to ensure asset protection, including:

    1- procedures to protect organizational assets, including information, software and hardware;
    2- any required physical protection controls and mechanisms;
    3- controls to ensure protection against malicious software;
    4- procedures to determine whether any compromise of the assets, e.g. loss or modification of information, software and hardware, has occurred;
    5- controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the agreement;
    6- confidentiality, integrity, availability, and any other relevant property of the assets;
    7- restrictions on copying and disclosing information, and using confidentiality agreements;

c. user and administrator training in methods, procedures, and security;
d. ensuring user awareness for information security responsibilities and issues;
e. provision for the transfer of personnel, where appropriate;
f. responsibilities regarding hardware and software installation and maintenance;
g. a clear reporting structure and agreed reporting formats;
h. a clear and specified process of change management;
i. access control policy, covering:

    1- the different reasons, requirements, and benefits that make the access by the third party necessary;
    2- permitted access methods, and the control and use of unique identifiers such as user IDs and passwords;
    3- an authorization process for user access and privileges;

4- a requirement to maintain a list of individuals authorized to use the services being made available, and what their rights and privileges are with respect to such use;
5- a statement that all access that is not explicitly authorized is forbidden;
6- a process for revoking access rights or interrupting the connection between systems;

j. arrangements for reporting, notification, and investigation of information security incidents and security breaches, as well as violations of the requirements stated in the agreement;
k. a description of the product or service to be provided, and a description of the information to be made available along with its security classification;
l. the target level of service and unacceptable levels of service;
m. the definition of verifiable performance criteria, their monitoring and reporting;
n. the right to monitor, and revoke, any activity related to the entity's assets;
o. the right to audit responsibilities defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors;
p. the establishment of an escalation process for problem resolution;
q. service continuity requirements, including measures for availability and reliability, in accordance with an entity's business priorities;
r. the respective liabilities of the parties to the agreement;
s. responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, e.g. data protection legislation, especially taking into account different national legal systems if the agreement involves co-operation with entities in other countries;
t. intellectual property rights (IPRs) and copyright assignment and protection of any collaborative work;
u. involvement of the third party with subcontractors, and the security controls these subcontractors need to implement;
v. conditions for renegotiation/termination of agreements:

1- a contingency plan should be in place in case either party wishes to terminate the relation before the end of the agreements;
2- renegotiation of agreements if the security requirements of the entity change;
3- current documentation of asset lists, licenses, agreements or rights relating to them.

M1.4	Support
Objective	To provide sufficient resources, appropriate communication and documentation for the Entity Information Security Program.
Performance Indicator	Percentage of incidents that are caused by a lack of qualified resources for information security.
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Insufficient resources • Non-compliance with information security controls • Incompetent information security personnel • Incomplete or not up to date documentation

M1.4.1	Resources	Priority	P1			
		Applicability	Always applicable			
Control	The entity shall determine and provide the appropriate resources needed for the entity's information security continual improvement					
Sub-Control	The entity shall ensure for the establishment, implementation, maintenance and continual improvement of its information security that: 1) The amount of human and financial resources provided shall be adequate for the work to be carried out for information security 2) The allocated human resources shall be sufficiently competent for their information security roles and responsibilities; the entity shall: a. determine the necessary competence of person(s) doing work under its control that affects its information security performance; b. ensure that these persons are competent on the basis of appropriate education, training, or experience; c. where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and d. retain appropriate documented information as evidence of competence					

Implementation Guidance (for information purpose only)

The entity should allocate appropriate resources for information security, taking account of:

a. people, skills, experience and competence;
b. resources needed for each part of the process to achieve and maintain information security;
c. specific resources for information security risk management (refer to M2);
d. documentation (refer to M1.4.3);
e. knowledge and management of competence; and
f. training programs (refer to M3.2).

Top management is responsible for ensuring that the right resources are allocated, and that all resources receive appropriate training. All personnel should have the competence to perform the operations required in the role assigned. The training performed should help all personnel be aware of and understand the meaning and importance of the information security activities they are involved in, and how they can contribute to achieving the objectives of information security.

M1.4.2	Internal and External Communication	Priority	P2
		Applicability	Always applicable
Control	The entity shall determine the plan and mechanism for internal and external communications in support of its information security.		
Sub-Control	1) The entity shall determine: a. on what to communicate b. when to communicate c. with whom to communicate d. who shall communicate e. the processes by which communication shall be effected 2) The entity shall ensure that adequate communication can be maintained with the designated UAE Government entities 3) The entity shall document the communication plan.		

Implementation Guidance (for information purpose only)

Internal communication: The entity should establish internal communication and reporting mechanisms in order to support information security. These mechanisms should ensure that:

a. key components of the information security controls, and any subsequent modifications, are communicated appropriately;
b. there is adequate internal reporting on information security, its effectiveness and the outcomes;
c. relevant information derived from the application of security controls is available in the entity, as appropriate; and
d. there are processes for consultation with internal stakeholders.

External communication: The entity should develop and implement a plan as to how it will communicate with external stakeholders. This should involve:

a. engaging appropriate external stakeholders and ensuring an effective exchange of information);
b. external reporting to comply with legal, regulatory, sector and governance requirements;
c. providing feedback and reporting on communication and consultation;
d. using communication to build confidence in the entity and its security; and
e. communicating with stakeholders in the event of a crisis or contingency.

During communication, care should be taken regarding the confidentiality of the information involved.

M1.4.3	Documentation	Priority	P2
		Applicability	Always applicable
Control	The entity shall maintain, protect and control documentation of its information security controls and their implementation.		
Sub-Control	The entity shall ensure that 1) documents are approved prior to issue 2) documents are reviewed and updated as necessary 3) changes and the current revision status of documents are identified 4) documents remain legible and readily identifiable 5) documents are available to those who need them, are transferred, and stored in accordance with the procedures applicable to their classification 6) documents are disposed of in accordance with the procedures applicable to their classification 7) documents of external origin are identified 8) the distribution of documents is controlled 9) the unintended use of obsolete documents is prevented, and that up to date versions are available 10) suitable identification is applied to documents if they are retained for any purpose The entity shall document the compliance with the "mandatory" controls in a way that allows unique reference to the requirements of this Regulation. (Sample Compliance Template may be provided by TRA in this regard).		

Implementation Guidance (for information purpose only)

One of the most important aspects of implementing document management in an entity is to do this consistent and throughout the entity, with supporting training, awareness and also checking that the document management controls are followed. It is necessary to include templates for document management in all documentation, irrespective of the form it takes.

All this can be supported by using document management systems and other controls to technically ensure that the necessary actions are carried out, wherever it is possible, it is recommended to use technical support to achieve a complete implementation.

Compliance with this control should be checked every so often, and non-compliances should be reacted to, to demonstrate that this actually is an important control everybody needs to comply with.

Particular attention should be given to the protection of records – it is not so important for records to have an author (they are often system based- and a change history (they should not change at all if they are supposed to provide evidence), but the date of issue and the integrity of the record are important items to maintain.

M2 Information Security Risk Management

M2	Information Security Risk Management
Objective	To ensure that information security risks in the entity are identified, assessed and -evaluated, and that these risks are treated in accordance with the information security requirements and objectives of the entity
Performance Indicator	Measure the percentage of risks that appear in the previous and the current risk assessment that have changed to a lower level Percentage of risks that appear in the previous and the current risk assessment that have changed to a higher level

M2.1	Information Security Risk Management Policy
Objective	To establish a formal information risk management framework for managing entity's information security risks by establishing the context, preforming risk assessment, implementing risk treatments, and monitoring their implementation
Performance Indicator	Trend in the number of occurrences where the risk assessment has not been performed, reviewed or updated as planned.
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Unsuitable risk management policy • Inconsistent or incomparable results • Inconsistent or unsuitable risk criteria

M2.1.1	Information Security Risk Management Policy	Priority	P1			
		Applicability	Always applicable			
Control	The entity shall establish a formal information security risk management policy.					
Sub-Control	The information security risk management policy shall: 1) take into account relevant TRA's issuances in regard to risk management 2) be documented and formally approved 3) addresses the purpose and scope of critical services and their supporting functions 4) categorize Information Asset based on its criticality 5) addresses roles and responsibilities of the risk assessment team involved 6) establish and maintain information security basic criteria, including the risk acceptance criteria, impact criteria, and risk evaluation criteria 7) contain a risk treatment strategy 8) contain a risk monitoring and review strategy 9) determine the criteria for performing, reviewing and updating information security risk assessments 10) ensure that repeated information security risk assessments produce consistent, valid and comparable results					

Implementation Guidance (for information purpose only)

Entities owning, operating, and or maintaining Critical Information Infrastructure shall take into account all relevant TRA's issuances and guidance with regard to risk management when performing risk assessment (Please refer to NCRMF for further details).

The information security risk management policy should clearly define how the entity is planning to carry out the risk assessment. In addition to the requirements stated above, the policy can, for example, contain:

a. the level of detail of asset identification;
b. the basis of threat and vulnerability identification;
c. the scales to be used for asset valuation in terms of confidentiality, integrity and availability;
d. how the likelihood that a threat exploits a vulnerability is calculated;
e. how the risks are calculated;
f. who will be responsible to perform the risk assessment;
g. the basis of control selection;
h. how to measure the risk management performance; and
i. criteria for improving the risk management.

The risk management policy should also describe the type of risk assessment the entity intends to perform, whether it is more of a higher level assessment or a detailed one (see also M2.2), and the reasons for that choice. The decision for a particular approach should be made based on

a. the security requirements of the entity;
b. their current level of maturity, and where the entity eventually wishes to be (link to self-assessment);
c. the capabilities, knowledge and resources available at this point in time; and
d. the given by the entity's sector or other applicable .

The entity should be able to provide reasons for the chosen information security risk management approach.

The risk management policy should be communicated appropriately.
Please note: the risk management policy is sometimes also denoted as risk management approach.

M2.2	Information Security Risk Assessment
Objective	To identify, analyze and evaluate the information security risks the entity is facing.
Performance Indicator	Percentage of new risks that are identified when the risk assessment is reviewed or updated in relation to all those risks that should have been identified before and have been overlooked or that have been assessed incorrectly.
Automation Guidance	Tools can be used for risk assessment and treatment; there are many tools on the market. When doing so, care should be taken to use a tool that is • suitable to the entity • complies with the requirements of these • allows to address all controls included in these • easy and effective to use The use of risk assessment tools can help in performing and updating the risk assessment and treatment.
Relevant Threats and Vulnerabilities	• Unidentified risks • Incorrect asset valuation • Threats or vulnerabilities that have not been considered • Wrongly assessed risks

M2.2.1	Information Security Risk Identification	Priority	P1
		Applicability	Always applicable
Control	The entity shall identify its information security risks.		
Sub-Control	The entity shall: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for its information by: • define the scope of the risk assessment exercise • identify critical business functions • identify critical information systems supporting business critical functions within the scope and boundary of the risk assessment • identifying vulnerabilities related to the information and information systems. (see also T 7.7) • identify existing information security controls • Identifying threats and threat sources 2) identify the risk owners 3) document the results of the risk identification.		

Implementation Guidance (for information purpose only)

There is a lot of information related to the performance of information security risk assessments; therefore, this implementation guidance will just provide an overview of the most important concepts. Entities should take into account relevant TRA's issuances and guidance with regard to risk management when performing risk assessment.

Level of detail of the information security risk assessment:
Some entities might find it difficult or time consuming to conduct a detailed risk assessment. The choice of a suitable risk management approach should be taken when drafting the Information Security Risk Management Policy (refer to M2.1.1), and the implementation guidance there explains the considerations the entity should take into account when deciding on a suitable way of doing information security risk management. The entity should document these results and should be able to provide reasons for the decision taken.

An entity will only be considered as being compliant with the requirements of this Regulation if they apply a suitable information security risk management policy.

Asset identification:
The assets to be considered in the information security risk assessment are all information assets, i.e. include:

a. information: databases, files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, etc.
b. software assets: application software, system software, development tools, and utilities
c. physical assets: computer equipment, communications equipment, removable media, and
d. other equipment
e. services: computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning

f. people, and their qualifications, skills, and experience
g. intangibles, such as reputation and image of the entity

The identified assets are summarized in the Asset Inventory (refer to T1.2.1).
It might be useful to summarize assets in suitable groups (e.g. all PCs in a call center, processing the same type of information), but care should be taken to only group "like with like" when doing so. It is also helpful to take account of business processes, as they often can help to understand the information flow and how assets are working in the entity.

Identification of threats:
Threats are not very dependent on the entity and its business; they are just out there trying to succeed. When identifying threats, it can be helpful to use threat lists (e.g. those provided in this Regulation, or in other standards, such as ISO/IEC 27005), and to look into incident reports (incidents are always related to threats that have been successful- and audit reports, and to keep an open mind to the latest development as new threats will continue to emerge.

It is also important to not only look at threats from the outside, such as hackers or malware, but also consider inside threats. A disgruntled employee with given access rights can often do more damage as outsiders.

Identification of vulnerabilities:
The identification of vulnerabilities should be based on an assessment of the existing controls. To do so, it is recommended to conduct a gap analysis, which checks the controls in place against this Regulation. The results of the gap analysis form an input in the identification of vulnerabilities as well as into the assessment of the risk likelihood (see also M2.2.2 below).

Any control, which has been identified as missing, not completely in place, not fully documented or not complied with identifies at least one (if not more- vulnerabilities, which might be exploited by the identified threats.

Please note: The identification of threats and vulnerabilities takes place per each identified asset, so this easily produces a lot of information. To keep the amount of information manageable, it is recommended to:

a. identify threats and vulnerabilities with the existing controls in mind
b. identify only threat/vulnerability pairs where the threat will actually exploit the vulnerability

See also T 7.7 on Technical Vulnerability Management

M2.2.2	Information Security Risk Analysis	Priority	P1			
		Applicability	Always applicable			
Control	The entity shall analyze its information security risks.					
Sub-Control	The entity shall: 1) assess the potential consequences that would result if the identified risks were to materialize by assessing the consequences of losses of confidentiality, integrity or availability 2) assess the realistic likelihood of the occurrence of the identified risks based on the existing controls, identified vulnerabilities and threats 3) determine the levels of risk 4) document the results of the risk analysis					

Implementation Guidance (for information purpose only)

There is a lot of information related to the performance of information security risk assessments, and more details will be provided in a separate risk management document, therefore, this implementation guidance will just provide an overview of the most important concepts.

Consequences of losses of confidentiality, integrity or availability: The first part of assessing the consequences of losses of confidentiality, integrity or availability is to identify the business importance the information asset under consideration has. Damage to an asset that is important for the business is much likelier to cause severe consequences than an asset that is not as important. Based on the business use of the asset, the consequences for a loss of the following needs to be assessed:

a. confidentiality – this means the information asset is only accessible to those authorized to access it
b. integrity – this means the information asset has not been modified in any unauthorized way
c. availability – this means the information asset is available, when needed

To make the results of this assessment comparable, scales should be used, which should have been defined in the Information Security Risk Management Policy (see M2.1.1 above).

The assessment of these consequences should be done together with the business users of the information assets, as these can give important input into the process because they are aware of the security requirements for their assets. This can be done by interviews and/or questionnaires, but it is important to ensure that the business users understand what is asked from them.

As a result, each asset should have identified consequences of losses of confidentiality, integrity and availability.

Likelihood of threat/vulnerability combinations: The input into the assessment of the likelihood that a particular threat exploits a vulnerability is based on very similar considerations as the identification of threats and vulnerabilities (see M2.2.1 above). The likelihood of a threat occurring can be derived from threat catalogues and statistics, as well as incident records, audit logs and reports, etc. the entity has produced.

The level of vulnerability is based on how good or bad the controls are that have been put in place, so this can also be derived from the results of the gap analysis (see M2.2.1 above). Finally, the likelihood of the threat to occur and the level of vulnerability are put together to determine the likelihood that this particular threat/vulnerability combination occurs. How exactly these values are put together has been defined in the Information Security Risk Management Policy (see M2.1.1. above).

Determining the levels of risk: Based on the method to calculate risks, which has been chosen by the entity and has been documented in the Information Security Risk Management Policy (see M2.1.1. above), the risks should now be calculated using the consequences and likelihoods that have been assessed.
Please note: The details on how to calculate the risks and which valuation schemes are used for consequences and likelihood is entirely up to the entity to decide. It is nevertheless important that the approach chosen is applied consistently.

M2.2.3	Information Security Risk Evaluation	Priority	P1			
		Applicability	Always applicable			
Control	The entity shall evaluate its information security risks.					
Sub-Control	The entity shall: 1) compare the analyzed risks with the risk criteria established in the information security risk management policy (See M2.1.1) 2) establish priorities for treatment of the identified risks 3) document the results of the risk evaluation and share with national and sector authorities, as required.					
Implementation Guidance (for information purpose only)						

There is a lot of information related to the performance of information security risk assessments, and more details will be provided in a separate risk management document, therefore, this implementation guidance will just provide an overview of the most important concepts.

Once the risks have been calculated (see M2.2.2 above), the entity should compare the risk levels assessed with the risk criteria that have been established documented in the Information Security Risk Management Policy (see M2.1.1. above). This will rank the risks in order of severity and will identify those that are acceptable (because they are below the general threshold of acceptance), and those risks that will require treatment.

If necessary, the entity can assign additional priorities to the risks, e.g. if a risk – despite of not being high- relates to a very vital business process. Any such assignment is entirely up to the entity, any decisions made should be reasoned and documented.

Decisions on risks should take account of the wider context of the risk and include consideration of the requirements of other parties, such as sector, regional or national initiatives. In some circumstances, the risk evaluation can lead to a decision to undertake further analysis.

M2.3	Information Security Risk Treatment
Objective	To identify and plan appropriate risk treatment for the risks that have been assessed.
Performance Indicator	Percentage of all records (audit reports, incident reports, logs, events, etc.) that indicate that any of the controls that have been identified as "not applicable" are actually needed.
Automation Guidance	See M2.2
Relevant Threats and Vulnerabilities	• Inadequately treated risks • Incomplete control selection • Too high residual risks • Wrongly assessed residual risks • Lack of management awareness of information security risks

M2.3.1	Information Security Risk Treatment Options	Priority	P1
		Applicability	Always applicable
Control	The entity shall select appropriate information security risk treatment options, taking account of the risk assessment results.		
Sub-Control	1) The entity shall consider the following risk treatment options and select one or more of them for each of the risks that have been assessed: • Risk Reduction – Reducing the risk by applying security controls • Risk Retention – Accepting the risk based on the entity's risk accepting criteria established on the information management risk policy (See M2.1.1) • Risk Avoidance – Avoiding the activity or condition causing th e risk • Risk Transfer – Transferring the risk to another party 2) The entity shall assess the risk treatment chosen to ensure that the selection of risk treatment options is successful by: • deciding whether residual risk levels are tolerable • if not tolerable, generating a new risk treatment • assessing the effectiveness of that treatment (see also M2.3)		

Implementation Guidance (for information purpose only)

Selecting the most appropriate information security risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, with regard to sector, national or regulatory requirements. Decisions should also take into account risks which can warrant risk treatment that is not justifiable on economic grounds, e.g. severe (high negative consequence- but rare (low likelihood- risks. A number of treatment options can and should be considered and applied either individually or in combination. When selecting risk treatment options, the entity should consider the expectations of the sector and national level. Though equally effective, some risk treatments can be more acceptable to some stakeholders than to others.

The selected risk treatment options should be documented in the risk treatment plan. The treatment plan should clearly identify the priority order in which individual risk treatments should be implemented. Risk treatment itself can introduce risks. A significant risk can be the failure or ineffectiveness of the risk treatment measures. Monitoring needs to be an integral part of the risk treatment plan to give assurance that the measures remain effective (see also M6).

M2.3.2	Identification of Controls	Priority	P1
		Applicability	Always applicable
Control	The entity shall identify all controls that are necessary to implement the information security risk treatment option(s) chosen.		
Sub-Control	The entity shall: 1) consider the controls included in these as a starting point for the control identification 2) ensure that no controls are overlooked by producing the Statement of Applicability (refer to M2.3.4) 3) identify controls in addition to the controls suggested in this Regulation that are specific to the entity 4) take account of the criteria for accepting risks (refer to M2.3.1) as well as legal, regulatory and contractual requirements when making the control selection.		

Implementation Guidance (for information purpose only)

Controls should be identified to manage the risks, based on the identified risk treatment option(s). It is important to specify the relation between the risks and the identified controls, this relation is important for the ongoing risk management and should be documented in the risk treatment plan.

The first basis of control identification should be this Regulation, which suggests a set of "risk-based applicable" controls that addresses a lot of the common information security risks. Sector-specific controls should be identified to support the specific needs of the entity within its sector.

The entity should also identify controls that are required for risk management and not documented in this Regulation. It is likely that such controls exist as an entity has risks specific to its business and its way to operate, and the identification of additional controls completes the controls for information security risk management.

The entity should compile a list of controls which have been identified to produce a Statement of Applicability (refer to M2.3.4). It might be that the Statement of Applicability (refer to Implementation Guidance of M2.3.4) leads to a revision of the identified controls. This is the intention of producing the Statement of Applicability, it is supposed to act as a safety net that ensures that no impotent control has been overlooked.

It is important to be aware of that the list of identified controls is very likely to contain sensitive information. Therefore, appropriate care should be taken when making the summary of controls available to both internal and external recipients.

M2.3.3	Risk Treatment Plan	Priority	P1
		Applicability	Always applicable
Control	The entity shall formulate a risk treatment plan.		
Sub-Control	1) The risk treatment plan shall identify: a. appropriate management actions b. resources required c. responsibilities and priorities for managing information security risks d. target dates for implementation of the identified controls 2) The entity shall document the risk treatment plan.		
Implementation Guidance (for information purpose only)			

The purpose of risk treatment plans is to document how the chosen risk treatment options will be implemented. The information provided in treatment plans should include:

a. the reasons for selection of treatment options;
b. the controls that have been identified to implement the selected risk treatment option(s);
c. the identified risk reduction or other modification that is intended to be achieved by the identified control(s), also called residual risk;
d. those who are accountable for approving the plan;
e. those responsible for implementing controls and the overall plan;
f. proposed actions to achieve this implementation;
g. priorities of implementation;
h. resource requirements including contingencies;
i. target dates for control implementation;
j. interdependencies of control implementation (when the implementation of a control requires the complete implementation of another control);
k. performance measures and constraints (which can also be documented elsewhere); and
l. reporting and monitoring requirements.

The risk treatment plan should be integrated with the management processes of the entity and discussed with appropriate stakeholders.

Management should be aware of the nature and extent of the residual risk after risk treatment and should accept the residual risks. The residual risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

M2.3.4	Statement of Applicability	Priority	P1
		Applicability	Always applicable
Control	The entity shall compare the controls identified in M2.3.2 above with the "risk-based applicable" controls contained in this Regulation and shall verify that no necessary controls have been omitted.		
Sub-Control	The entity shall produce and document a Statement of Applicability that contains: 1) the controls that have been identified as necessary 2) reasons for identification of these controls 3) their current status of implementation 4) justification for exclusion of any of the "risk-based applicable" controls contained in these		

Implementation Guidance (for information purpose only)

The Statement of Applicability should be produced to ensure that no control from these that is required by the entity for risk treatment is overlooked.

If the first version of the Statement of Applicability identifies controls from this Regulation whose exclusion cannot be justified, the entity should go back to the control identification process (refer to M2.3.2) and check whether there are risks whose treatment could benefit from this control. If this is the case, the control under consideration should be included in the risk treatment. If this is not the case, the entity should go back to the risk identification and ensure that all important risks have been identified.

The reasons for the identification of controls is needed to form the link between risks and controls – this relationship can also be documented in the risk treatment plan (refer to M2.3.3). The Statement of Applicability can be a separate document, or can be combined with the risk treatment plan, this can be decided by the entity.

M2.3.5	Information Security Objectives	Priority	P2
		Applicability	Always applicable
Control	The entity shall establish information security objectives at relevant to its functions and levels.		
Sub-Control	1) The information security objectives shall: a. be consistent with the information security policy b. be measurable (if practicable) c. take into account applicable information security requirements, and risk assessment and treatment results d. be communicated within the entity e. be updated as appropriate f. be documenteda.		

Implementation Guidance (for information purpose only)

Based on the business objectives for information security and the results of the information security risk assessment and risk treatment process, information security objectives should be identified. The entity can consider high level objectives, such as:

a. maintaining the confidentially of sensitive entity information
b. successful management of the information security risks
c. efficient management of information security in the entity
d. compliance with sector or national requirements

These high level information security objectives are often directly derived from the business objectives, and other, lower level objectives, can be identified to support their fulfillment. The lower level information security objectives can be identified based on the results of the information security risk assessment and risk treatment process, and can also be identified by considering the following questions:

a. What third party relationships and agreements exist, and what are associated information security requirements?
b. Are there any services that have been outsourced?
c. What kind of protection is needed, and against what threats?
d. What are the distinct categories of information that require protection?
e. What are the distinct types of information activities that need to be protected?
f. What are the minimum market requirements for information security?
g. What additional information security controls should provide a competitive advantage for the entity?
h. What are the critical business processes, and how long can the entity tolerate interruptions to each icritical business process?

When planning how to achieve the information security objectives, it can be helpful to develop an equivalent of the risk treatment plan, i.e. a plan that details the actions, resources, responsibilities, time frames and methods of evaluating whether the objectives have been achieved.

When planning how to achieve its information security objectives, the entity shall determine:

a. what will be done
b. what resources will be required
c. who will be responsible
d. when it will be completed
e. how the results will be evaluated

M2.4	Ongoing Information Security Risk Management
Objective	To ensure that risk management process is communicated, consulted and monitored.
Performance Indicator	Percentage of all cases during the last year where the information security risk assessment and/or risk treatment has not been updated despite of being scheduled and significant changes are occurring
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• No review or update of the information security risk assessment and treatment • Unidentified new information security risks • Unnecessary controls

M2.4.1	Information Security Risk Assessment Review and Update	Priority	P1
		Applicability	Always applicable
Control	The entity shall plan and document the process for the review and update of the risk assessment and treatment; this shall include planned reviews and updates as well as ad hoc updates if significant changes occur.		
Sub-Control	1) The entity's monitoring and review processes shall encompass all aspects of the risk management process and shall take account of changes in: a. the entity itself b. technology used c. business objectives and processes d. risk criteria and the risk assessment process e. assets and consequences of losses of confidentiality, integrity or availability f. identified threats; g. identified vulnerabilities h. effectiveness of the implemented controls i. external events, such as changes to the legal or regulatory environment, changed contractual obligations, and changes in social climate 2) the entity shall monitor security incidents (see T8.3.2, T8.3.3) that might trigger the risk assessment process. (see M2.2.1) 3) Responsibilities for monitoring and review shall be clearly defined and documented.		

Implementation Guidance (for information purpose only)

Monitoring and review should be a planned part of the information security risk management process and involve regular checking, surveillance and updates. The monitoring should be an ongoing process, which identifies any changes that are relevant to information security risk management, and there should also be planned processes that ensure that risk assessment and treatment updates are taking place.

Responsibilities for monitoring and review should be clearly defined. (Refer to NCRMF for further details) The entity's monitoring and review processes should encompass all aspects of the information security risk management process for the purposes of:

a. ensuring that controls are effective in the risk management they are achieving
b. integrating new information to improve the risk assessment and/or treatment
c. analyzing and learning lessons from events (including near-misses), changes, trends, successes and failures;
d. detecting changes in the external and internal context, including changes to risk criteria and the risk itself, which can require revision of risk treatments and priorities
e. Vulnerability Assessment should be conducted frequently even after implementing security controls to identify emerging risks, new threats, trends, etc.

Progress in implementing risk treatment plans provides a performance indicator in itself. The results can be incorporated into the entity's overall performance management, measurement and external and internal reporting activities.

The results of monitoring and review should be recorded and externally and internally reported as appropriate, and should also be used as an input to the review of the information security risk management policy (refer to M2.1.1).

M2.4.2	Risk Communication and Consultation	Priority	P1
		Applicability	Always applicable
Control	The entity shall communicate and consult risk information obtained from risk management activities with all stakeholders involved.		
Sub-Control	The entity shall: 1) establish a risk communication plan for communicating risk information with key stakeholders including decision-makers within the entity during all stages of the risk management process 2) take into account all TRA's issuances with regard to risk management		

Implementation Guidance (for information purpose only)

Communication and consultation with key stakeholders should take place during all stages of the risk management process. Therefore, plans for communication and consultation should be developed at an early stage. These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Effective external and internal communication and consultation should take place to ensure that stakeholders and those accountable for implementing the risk management process understand the basis on which decisions are made, as well as the reasons why particular actions are required.

M3 Awareness and Training

M3	Awareness and Training
Objective	To ensure sufficient information security awareness and training is provided and to build a specialized workforce
Performance Indicator	Percentage of awareness and training objectives that have been met successfully

M3.1	Awareness and Training Policy
Objective	To maintain an awareness and training policy outlining the approach to identifying relevant topics, enrollment of stakeholders, and documentation of activities
Performance Indicator	Trend in the number of employees that have not successfully participated in the awareness and training program.
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Unsuitable awareness and training policy • Non-comprehensive training identification approach • Accidental information leaks due to lack of awareness • Software malfunction due to lack of trained personnel

M3.1.1	Awareness and Training Policy	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall develop and maintain an awareness and training policy.		
Sub-Control	The awareness and training policy shall: 1) be appropriate to the purpose of the entity 2) provide the framework for setting awareness and training objectives 3) facilitate the implementation of the associated controls 4) outline the roles and responsibilities of providers and recipients of awareness and training activities		

Implementation Guidance (for information purpose only)

Critical entities shall also take into account TRA's relevant issuances, guidance, and activities with regards to National Awareness and Capability Building.
The policy document should contain statements concerning:

a. the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
b. the procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls
c. factors to consider when awareness and training objectives are identified

M3.2	Awareness and Training Planning
Objective	To ensure that all person(s) carrying out work effecting information security are sufficiently aware of information security requirements and controls, and are adequately competent.
Performance Indicator	Percentage of actions (planned training, participation in conferences, etc.) that have not been carried out as planned.
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Non-compliance with controls due to a lack of awareness • Not noticing security breaches • Incompetent information security personnel • Promoting a culture of disinterest in information security matters

M3.2.1	Awareness and Training Program	Priority	P2
		Applicability	Always applicable
Control	The entity shall develop an awareness and training program.		
Sub-Control	The awareness and training program shall: 1) inform persons doing work under the entity of their contribution to the effectiveness of information security and the implications of not conforming to the information security requirements The entity shall: 2) determine the necessary competencies for personnel performing work effecting information security 3) provide training or taking other actions (e.g. employing competent personnel) to satisfy these needs 4) evaluate the effectiveness of the actions taken 5) maintain records of education, training, skills, experience and qualifications		
Implementation Guidance (for information purpose only)			

Critical entities shall also take into account TRA's national awareness and capability building issuances, guidance, and activities.

The entity should develop a program that ensures continued adequate awareness and competence for all persons doing work under the control of the entity. This does include not only entity personnel but also any outsiders with access to information. Please note that the implementation of the awareness and training program might not be carried out by the entity and can, for example, be ensured contractually. The first step in the program is the evaluation of the competencies required for the job function. The Information Security Manager, for example, should have a good understanding of the controls contained in this Regulation, and should know how to implement them and to maintain them effectively.

The entity should ensure that trainings take place as planned, and are not pushed off, e.g. due to work overload. If such problems recur, it might be a sign for inadequate resourcing. If trainings continue not to take place in the time frame planned, it is a non-conformity to sub-control 2- mentioned above.

The awareness and training program should ensure that records of all trainings are generated. These records should regularly be reviewed to ensure that all personnel have received the training that they require.

Whatever training is conducted, it is important that the effectiveness of this training is assessed. An easy way of such as assessment is to select trainings that include an exam at the end. Whenever this is not possible, interviews of feedback form should be used that provide enough information to be able to evaluate the effectiveness of the training.

M3.3	Security Training
Objective	To ensure that all personnel who are assigned responsibilities in information security are competent to perform the required tasks
Performance Indicator	Percentage of identified information security training requirements that have been met with satisfactory results
Automation Guidance	Web-based training modules (internally or externally created) can be used to implement trainings. This can also be used to automatically update staff training records, as well as to capture CPE credits needed to maintain security certifications.
Relevant Threats and Vulnerabilities	• Software malfunction due to lack of trained personnel • Error in use due to undelivered training

M3.3.1	Training Needs	Priority	P1
		Applicability	Always applicable
Control	The entity shall identify its information security training needs.		
Sub-Control	The entity shall: 1) identify the information security skills needed within the entity 2) assess the current information skills in place within the entity 3) identify gaps between required and in place information security skills		

Implementation Guidance (for information purpose only)

Entities determine the appropriate content of security training and techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content should also include advanced security information for the implementation and maintenance of information assets deployed within the entity.

M3.3.2	Implementation Plan	Priority	P3
		Applicability	Always applicable
Control	The entity shall establish a clear plan to conduct the trainings needed for the corresponding target audience.		
Sub-Control	The entity shall: 1) Identify solutions for each information security training need that has been identified 2) Develop a timeline for delivering the information security training solutions 3) Ensure resources needed to execute information security training are allocated to the program		

Implementation Guidance (for information purpose only)

Entities should determine the trainings that should be delivered, the medium (class based, web based, documents), the target audience, and develop the corresponding timeline for the execution in line with known organizational and users' constraints.

M3.3.3	Training Execution	Priority	P2
		Applicability	Always applicable
Control	The entity shall conduct security training following an established plan.		
Sub-Control	The entity shall: 1) ensure that information security training proceeds according to the implementation plan 2) identify alternative information security training solutions if problems with the implementation plan arise 3) ensure the updated implementation plan satisfies all of the information security training needs identified		

Implementation Guidance (for information purpose only)

Security trainings typically focus on topics specific to the applications and systems within the entities, such as security best practices for implementing and maintaining a database or patching operating systems. Specific training methods may include:

a. internal training websites;
b. manuals, guides, and handbooks;
c. slide presentations.

Entities should update training based on changes within the IT landscape, such as changing technology, updated systems, new services, or new threats.

M3.3.4	Training Results	Priority		P2		
		Applicability	Based on risk assessment			
Control	The entity shall measure and evaluate security training effectiveness.					
Sub-Control	The entity shall: 1) measure the level of information security knowledge and skills in the entity before and after the training plan is implemented 2) ensure that the information security training solutions implemented are meeting the expected outcomes against the knowledge requirements of the entity 3) take corrective action to improve or replace training solutions that are not reaching the expected outcome					
Implementation Guidance (for information purpose only)						

Effectiveness of training could be measured through:

a. written individual assessment of the training
b. voluntary self-reporting of participants
c. interviews
d. measurement of enhanced individual performance
e. compare events and incidents in the entity with training provided

M3.3.5	Records Documentation	Priority		P2		
		Applicability	Based on risk assessment			
Control	The entity shall maintain training records of all security personnel.					
Sub-Control	The entity shall: 1) ensure that each target for information security training has a documented training record 2) ensure that all training activities are captured in the individual training records containing personnel education, training, skills, experience and qualifications 3) review training records periodically to ensure all stakeholders have completed the necessary training					
Implementation Guidance (for information purpose only)						

The entity should consider the following:

a. document and monitor individual information system security training activities including basic security awareness training and specific information system security training; and
b. retain individual training records in line with the training and awareness policy.

M3.4	Security Awareness
Objective	To foster security awareness of the workforce within the entity
Performance Indicator	Percentage of identified Information Security campaigns that have been successfully implemented
Automation Guidance	Leverage internally or externally created web-based awareness modules to allow recurring training by the general workforce and external stakeholders. This can also be used to automatically update workforce training records.
Relevant Threats and Vulnerabilities	• Successful pretexting due to lack of awareness • Accidental leaks of data by staff • Illegal processing of data

M3.4.1	Awareness Campaign	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall plan and conduct a security awareness campaign.		
Sub-Control	The entity shall: 1) define the scope of the awareness campaign in terms of targets and content based on security risks relevant to users' activities 2) provide a timeline for deploying specific awareness campaigns to meet the program objectives 3) ensure that information security campaigns proceed according to the defined program timeline 4) identify alternative information security awareness campaigns if problems with the program timeline arise 5) ensure the updated information security awareness campaign satisfies all of the program objectives and needs identified		

Implementation Guidance (for information purpose only)

Through awareness campaigns, the entity promotes a culture of security. Security awareness programs typically focus on broad topics, such as security threats that could be mitigated through good practice, the choice and usage of passwords, good practice for using a personal computer, sharing of account information, report incidents.

Entities determine the appropriate content of security awareness based on the specific organizational requirements and the information systems to which personnel have authorized access. Specific training methods may include:

a. mandatory annual awareness training;
b. targeted, role-based training;
c. internal security awareness websites;
d. manuals, guides, and handbooks;
e. seminars and slide presentations;

f. events (e.g., security awareness week or month);
g. posters and brochures; and
h. email messages to all employees and contractors.

Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

M4 Human Resources Security

M4	Human Resources Security
Objective	To ensure stakeholder awareness of information security threats as well as their roles and responsibilities before, during and in post-employment scenarios
Performance Indicator	Percentage of employees, contractors and third parties who read and accepted human resources security policy

M4.1	Human Resources Security Policy
Objective	To maintain a human resources security policy covering the security aspects of employment and termination, in addition to the inclusion of information security in the job junction
Performance Indicator	Extent of HR security policy deployment and adoption across the entity Number of employees, contractors and third parties who have accepted the HR security policy and have denoted this acceptance in writing
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Unawareness of the human resources security policy • Non-compliance with human resources security policy • Intentional leaks and sharing of data by staff

M4.1.1	Human Resources Security Policy	Priority	P2
		Applicability	Always applicable
Control	The entity shall develop and maintain a human resources security policy and associated security controls.		
Sub-Control	The entity shall: 1) establish and maintain a human resources security policy that outlines roles and responsibilities of different stakeholders, and procedures to facilitate the implementation of the associated controls. 2) identify and implement associated controls		

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard.

The human resources security policy facilitates the implementation of the associated controls along the entire employment lifecycle: prior to employment, during employment, and termination or change of employment. The policy can, for example, contain:

a. Scope of the policy
b. Management roles and responsibilities during each phase of the employment lifecycle
c. Employment terms and conditions
d. Required information security awareness and training during employment in line with M3.1.1
e. Employment termination procedures and checks

The human resources policy can be included as part of the general information security policy, in a single policy document, or can be represented by multiple policies reflecting the complex nature of certain entities.

M4.2	Prior to Employment
Objective	To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities
Performance Indicator	Percentage of new employees and contractors that have been fully screened and approved in accordance with company policies prior to starting work Percentage of employees, contractors and third parties who read and accepted HR security policy
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Intentional leaks and sharing of data by staff • Successful pretexting due to unsuitability of new employee • Pretexting

M4.2.1	Screening	Priority	P2
		Applicability	Always applicable
Control	The entity shall perform background verification checks on all candidates for employment, contractors, and third party users		
Sub-Control	The entity shall: 1) define a background verification check process in accordance with relevant laws, and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks 2) perform background verification checks for all candidates for employment, contractors and third party personnel		

Implementation Guidance (for information purpose only)

Verification checks should take into account all relevant privacy, protection of personal data and/or employment based legislation, and should, where permitted, include the following:

a. availability of satisfactory character references, e.g. one business and one personal;
b. a check (for completeness and accuracy) of the applicant's curriculum vitae;
c. confirmation of claimed academic and professional qualifications;
d. independent identity check (passport or similar document);
e. more detailed checks, such as credit checks or checks of criminal records.

Where a job, either on initial appointment or on promotion, involves the person having access to information systems, and in particular if these are handling sensitive information, e.g. financial information or highly confidential information, the entity should also consider further, more detailed checks.

Procedures should define criteria and limitations for verification checks, e.g. who is eligible to screen people, and how, when and why verification checks are carried out.

A screening process should also be carried out for contractors, and third party users. Where contractors are provided through an agency the contract with the agency should clearly specify the agency's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern. In the same way, the agreement with the third party should clearly specify all responsibilities and notification procedures for screening.

Information on all candidates being considered for positions within the entity should be collected and handled in accordance with any appropriate legislation existing in the relevant jurisdiction. Depending on applicable legislation, the candidates should be informed beforehand about the screening activities.

M4.2.2	Terms and Conditions of Employment	Priority	P2
		Applicability	Always applicable
Control	The entity shall ensure that employees, contractors and third party user understand, agree and sign the terms and conditions of their employment contract, which should state their and the entity's responsibilities for information security, as part of their contractual obligation.		
Sub-Control	The entity shall: 1) define standard information security terms and conditions for employees, third parties and contractors 2) include information security terms and conditions in any contract 3) ensure that their employees, contractors, and third parties fully understand their relevant terms and conditions 4) review and eventually amend any existing contract with employees, contractors and third parties		

Implementation Guidance (for information purpose only)

The terms and conditions of employment should reflect the entity's security policy in addition to clarifying and stating:

a. that all employees, contractors and third party users who are given access to sensitive information should sign a confidentiality or non-disclosure agreement prior to being given access to information systems;
b. the employee's, contractor's and any other user's legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation;
c. responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the employee, contractor or third party user;
d. responsibilities of the employee, contractor or third party user for the handling of information received from other companies or external parties;
e. responsibilities of the entity for the handling of personal information, including personal information created as a result of, or in the course of, employment with the entity;
f. responsibilities that are extended outside the entity's premises and outside normal working hours, e.g. in the case of home-working;
g. actions to be taken if the employee, contractor or third party user disregards the entity's security requirements.

The entity should ensure that employees, contractors and third party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the entity's assets associated with information systems and services.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment.

M4.3	During Employment
Objective	To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error
Performance Indicator	Percentage of employees that participated in Security Awareness Training
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Abuse of system access/privileges • Use of unapproved hardware/devices • Illegal processing of data

M4.3.1	Management Responsibilities	Priority	P2
		Applicability	Always applicable
Control	The entity's management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the entity.		
Sub-Control	The entity shall: 1) include in human resources security policy that employees, contractors and third party users have to comply with entity security policies and procedures 2) inform all employees, contractors and third parties of the security policies they are required to be compliant with 3) present, on first access, relevant security policy/guidelines for users to read and accept		

Implementation Guidance (for information purpose only)

Management responsibilities should ensure that employees, contractors and third party users:

a. are properly briefed on their information security roles and responsibilities prior to being granted access to sensitive information or information systems;
b. are provided with guidelines to state security expectations of their role within the entity;
c. are motivated to fulfill the security policies of the entity;
d. achieve a level of awareness on security relevant to their roles and responsibilities within the entity;
e. conform to the terms and conditions of employment, which includes the entity's information security policy and appropriate methods of working;
f. continue to have the appropriate skills and qualifications.

M4.3.2	Disciplinary Process	Priority	P2
		Applicability	Always applicable
Control	The entity shall enforce a formal disciplinary process for employees who have committed a security breach.		
Sub-Control	The entity shall: 1) define a formal disciplinary process 2) ensure sufficient awareness about this disciplinary process within the entity 3) enforce the disciplinary process 4) keep records of the committed security breaches		

Implementation Guidance (for information purpose only)

The disciplinary process should not be commenced without prior verification that a security breach has occurred.

The formal disciplinary process should ensure correct and fair treatment for employees who are suspected of committing breaches of security. The formal disciplinary process should provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required. In serious cases of misconduct the process should allow for instant removal of duties, access rights and privileges, and for immediate escorting out of the site, if necessary

M4.4	Termination or Change of Employment
Objective	To ensure that employees, contractors and third party users exit an entity or change employment in an orderly manner
Performance Indicator	Percentage employees, contractors and third party user accounts that are blocked after termination Percentage of employees, contractors and third party users accounts which profiles are modified based on role change
Automation Guidance	An identity management system could be used to automatically disable terminated employee accounts and identify user accounts that are inactive
Relevant Threats and Vulnerabilities	• Abuse of system access/privileges • Intentional leaks and sharing of data by staff • Illegal processing of data

M4.4.1	Termination Responsibilities	Priority	P1			
		Applicability	Always applicable			
Control	The entity shall clearly define and assign responsibilities for performing employment termination or change of employment.					
Sub-Control	The entity shall: 1) define an employee termination policy that emphasizes the communication of termination responsibilities in relation to entities information security (including confidentiality and property rights) 2) assign responsibility for performing termination or change of employment					
Implementation Guidance (for information purpose only)						

The communication of termination responsibilities should include ongoing security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement, and the terms and conditions of employment continuing for a defined period after the end of the employee's, contractor's or third party user's employment.

Responsibilities and duties still valid after termination of employment should be contained in employee's, contractor's or third party user's contracts.

Changes of responsibility or employment should be managed as the termination of the respective responsibility or employment, and the new responsibility or employment should be controlled.

M4.4.2	Return of Assets	Priority	P1
		Applicability	Always applicable
Control	The entity shall ensure that all stakeholders should return all of the entity's assets in their possession upon termination of their employment, contract or agreement.		
Sub-Control	The entity shall: 1) include in employee termination policy that all employees, contractors and third parties should return of all assets upon termination of employment, contract or agreement		
Implementation Guidance (for information purpose only)			

The termination process should be formalized to include the return of all previously issued software, corporate documents, and equipment. Other organizational assets such as mobile computing devices, credit cards, access cards, software, manuals, and information stored on electronic media also need to be returned.

In cases where an employee, contractor or third party user purchases the entity's equipment or uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the entity and securely erased from the equipment.

In cases where an employee, contractor or third party user has knowledge that is important to ongoing operations, that information should be documented and transferred to the entity.

M4.4.3	Removal of Access Rights	Priority	P1
		Applicability	Always applicable
Control	The entity shall remove access rights of all stakeholders to information and information systems upon termination of their employment, contract or agreement, or adjusted upon change.		
Sub-Control	The entity shall: 1) verify that the termination policy and procedure is followed for any termination or change of employment, contract or agreement with particular attention to revocation of credentials/access to any information facility		
Implementation Guidance (for information purpose only)			

Upon termination, the access rights of an individual to assets associated with information systems and services should be reconsidered. This will determine whether it is necessary to remove access rights. Changes of an employment should be reflected in removal of all access rights that were not approved for the new employment. The access rights that should be removed or adapted include physical and logical access, keys, identification cards, information systems, subscriptions, and removal from any documentation that identifies them as a current member of the entity. If a departing employee, contractor or third party user has known passwords for accounts remaining active, these should be changed upon termination or change of employment, contract or agreement.

Access rights for information assets and information systems should be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors such as:

a. whether the termination or change is initiated by the employee, contractor or third party user, or by management and the reason of termination;
b. the current responsibilities of the employee, contractor or any other user;
c. the value of the assets currently accessible.

M5 Compliance

M5	Compliance
Objective	To ensure an entity is meeting all applicable requirements for information security
Performance Indicator	Percentage of audit findings that are repeated

M5.1	Compliance Policy
Objective	To maintain a compliance policy, which is outlining the legal, technical, and management security requirements that the entity needs to adhere to
Performance Indicator	Extent of compliance policy deployment and adoption across the entity
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Unsuitable compliance policy • Unawareness of compliance policy among staff

M5.1.1	Compliance Policy	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall develop and maintain a compliance policy with which the entity must be compliant at the entity, sector, and national levels.		
Sub-Control	The compliance policy shall: 1) be appropriate to the purpose of the entity 2) outline the roles and responsibilities for establishing compliance requirements 3) outline the approach for establishing compliance requirements 4) outline the approach the entity will follow to ensure compliance with the identified requirements at the entity, sector, and national levels		

Implementation Guidance (for information purpose only)

The compliance policy facilitates the implementation of the associated controls to ensure the entity is compliant at the entity, sector, and national levels. The policy includes applicable requirements, such as:

a. Information security legal requirements
b. Technical requirements
c. Non-technical requirements

In addition, the compliance policy typically outlines the considerations for information systems audit.

The compliance policy can be included as part of the general information security policy, in a single policy document, or can be represented by multiple policies reflecting the complex nature of certain entities.

M5.2	Compliance with Information Security Legal Requirements
Objective	To avoid breaches of any information security legal, statutory, regulatory or contractual obligations
Performance Indicator	Amount of time and resources spent by the legal department managing legal compliance issues with relation to information security
Automation Guidance	Compliance automation tools are available for entities of all sizes and complexity. Selection of the appropriate compliance automation tool requires an entity to understand its regulatory environment, the risks it faces, and the maturity levels of its own compliance staff.
Relevant Threats and Vulnerabilities	• Breaches of legal requirements • Unawareness of legal requirements • Inaccurate identification of legal requirements

M5.2.1	Identification of Applicable Legislation	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall define, document and maintain all applicable legislation's (including statutory, regulatory, and contractual) compliance requirements with relation to information security and the entity's approach to meet these requirements.		
Sub-Control	The entity shall: 1) develop a process to identify on an ongoing basis all compliance requirements applicable to the entity 2) determine specific system requirements resulting from the identified compliance requirements 3) define specific controls to ensure all compliance requirements are met 4) periodically review compliance requirements and associated controls for completeness 5) document all legislation requirements with individual responsibilities to meet these requirements as well as controls in-place		

Implementation Guidance (for information purpose only)

Applicable legislation for compliance consideration includes, but is not limited to, applicable federal laws, directives, , policies, standards, and other guidance.

The specific controls and individual responsibilities to meet these requirements should be similarly defined and documented.

M5.2.2	Intellectual Property Rights (IPR)	Priority	P4
		Applicability	Based on risk assessment
Control	The entity shall implement the appropriate procedures to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.		
Sub-Control	The entity shall: 1) develop and maintain an intellectual property rights compliance policy 2) develop a process to identify all applicable requirements the entity must meet in terms of protecting intellectual property rights 3) determine specific system requirements resulting from the identified requirements 4) define specific controls to ensure all intellectual property right protection requirements are met 5) periodically review requirements and associated controls for completeness		

Implementation Guidance (for information purpose only)

The following guidelines should be considered to protect any material that may be considered intellectual property:

a. publishing an intellectual property rights compliance policy which defines the legal use of software and information products;
b. acquiring software only through known and reputable sources, to ensure that copyright is not violated;
c. maintaining awareness of policies to protect intellectual property rights, and giving notice of the intent to take disciplinary action against personnel breaching them;
d. maintaining appropriate asset registers, and identifying all assets with requirements to protect intellectual property rights;
e. maintaining proof and evidence of ownership of licenses, master disks, manuals, etc.;
f. implementing controls to ensure that any maximum number of users permitted is not exceeded;
g. carrying out checks that only authorized software and licensed products are installed;
h. providing a policy for maintaining appropriate license conditions;
i. providing a policy for disposing or transferring software to others;
j. using appropriate audit tools;
k. complying with terms and conditions for software and information obtained from public networks;
l. not duplicating, converting to another format or extracting from commercial recordings (film, audio- other than permitted by copyright law;
m. not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law

M5.2.3	Protection of Organizational Records	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall protect important records from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.		
Sub-Control	The entity shall: 1) define a process for identifying records with specific compliance requirements regarding loss, destruction, falsification, or other applicable characteristics 2) determine specific system requirements resulting from the identified requirements 3) define specific controls to ensure all record protection requirements are met 4) periodically review requirements and associated controls for completeness		

Implementation Guidance (for information purpose only)

Records should be categorized into record types, e.g. accounting records, database records, transaction logs, audit logs, and operational procedures, each with details of retention periods and type of storage media. Any related cryptographic keying material and programs associated with encrypted archives or digital signatures, should also be stored to enable decryption of the records for the length of time the records are retained.

Consideration should be given to the possibility of deterioration of media used for storage of records. Storage and handling procedures should be implemented in accordance with manufacturer's recommendations. For long term storage, the use of paper and microfiche should be considered. Where electronic storage media are chosen, procedures to ensure the ability to access data (both media and format readability) throughout the retention period should be included, to safeguard against loss due to future technology change.

Data storage systems should be chosen such that required data can be retrieved in an acceptable timeframe and format, depending on the requirements to be fulfilled.

The system of storage and handling should ensure clear identification of records and of their retention period as defined by national or regional legislation or , if applicable. This system should permit appropriate destruction of records after that period if they are not needed by the entity.

To meet these record safeguarding objectives, the following steps should be taken within an entity:

a. guidelines should be issued on the retention, storage, handling, and disposal of records and information;
b. a retention schedule should be drawn up identifying records and the period of time for which they should be retained;
c. an inventory of sources of key information should be maintained;
d. appropriate controls should be implemented to protect records and information from loss, destruction, and falsification.

M5.2.4	Data Protection and Privacy of Personal Information	Priority	P3
		Applicability	Based on risk assessment
Control	The entity shall ensure data protection and privacy as required in relevant legislation, , and, if applicable, contractual clauses.		
Sub-Control	The entity shall: 1) define a process for identifying data with specific compliance requirements regarding protection and privacy 2) determine specific system requirements resulting from the identified requirements 3) define specific controls to ensure all data protection and privacy requirements are met 4) periodically review requirements and associated controls for completeness		

Implementation Guidance (for information purpose only)

An organizational data protection and privacy policy should be developed and implemented. This policy should be communicated to all persons involved in the processing of personal information.

Compliance with this policy and all relevant data protection legislation and requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a data protection officer, who should provide guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that should be followed.

Responsibility for handling personal information and ensuring awareness of the data protection principles should be dealt with in accordance with relevant legislation and . Appropriate technical and organizational measures to protect personal information should be implemented.

M5.2.5	Prevention of Misuse of Information Systems	Priority	P3
		Applicability	Based on risk assessment
Control	The entity shall deter users from using information systems for unauthorized purposes.		
Sub-Control	The entity shall: 1) clearly communicate to all stakeholders what is considered to be authorized use of information systems 2) develop the capability to monitor information systems for unauthorized use 3) take corrective action to stop unauthorized use of information systems when detected		

Implementation Guidance (for information purpose only)

Management should approve the use of information systems. Any use of these facilities for non-business purposes without management approval, or for any unauthorized purposes, should be regarded as improper use of the information systems. If any unauthorized activity is identified by monitoring or other means, this activity should be brought to the attention of the individual manager concerned for consideration of appropriate disciplinary and/or legal action.

Legal advice should be taken before implementing monitoring procedures. All users should be aware of the precise scope of their permitted access and of the monitoring in place to detect unauthorized use. This can be achieved by giving users written authorization, a copy of which should be signed by the user and securely retained by the entity. Employees of an entity, contractors, and third party users should be advised that no access will be permitted except that which is authorized.

At log-on, a warning message should be presented to indicate that the information systems being entered are owned by the entity and that unauthorized access is not permitted. The user has to acknowledge and react appropriately to the message on the screen to continue with the log-on process.

M5.2.6	Regulation of Cryptographic Controls	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall use cryptographic controls in compliance with all relevant legislations, , and agreements.		
Sub-Control	The entity shall: 1) define a process for identifying applicable compliance requirements regarding use of cryptographic controls within the entity 2) determine specific system requirements resulting from the identified requirements 3) define specific controls to ensure all cryptographic control requirements are met 4) periodically review requirements and associated controls for completeness		

Implementation Guidance (for information purpose only)

The following items should be considered for compliance with the relevant legislations, , and agreements:

a. restrictions on import and/or export of computer hardware and software for performing cryptographic functions;
b. restrictions on import and/or export of computer hardware and software which is designed to have cryptographic functions added to it;
c. restrictions on the usage of encryption;
d. mandatory or discretionary methods of access by the countries' authorities to information encrypted by hardware or software to provide confidentiality of content.

Legal advice should be sought to ensure compliance with national laws and . Before encrypted information or cryptographic controls are moved to another country, legal advice should also be taken.

M5.2.7	Liability to the Information Sharing Community	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity shall ensure that liability issues and remediation are clarified, understood and approved by all members of an information sharing community, to address situations in which information is intentionally or unintentionally disclosed.					
Sub-Control	The entity shall: 1) identify any liability issues and remediation requirements regarding unauthorized disclosure of information in all information sharing communities in which the entity participates 2) define specific remediation procedures for each relevant information sharing community 3) communicate to the relevant information sharing community any issues identified regarding remediation procedures					

Implementation Guidance (for information purpose only)

Remediation should include, at a minimum, notification of any unauthorized disclosure back to the originator, with sufficient detail to identify the information disclosed.

Where possible, notification should be provided back to the source, even if the information has been sanitized and does not reveal its origin. This could be achieved by the intermediary of a trusted third party.

Unauthorized disclosure consequences could affect directly the responsible parties and might involve eliminating or restricting access to some members for some period of time to re-establish community trust.

M5.3	Compliance with non-technical requirements
Objective	To ensure compliance with the entity's information security policies and standards
Performance Indicator	Percentage of information security management sub-controls that have been implemented
Automation Guidance	Compliance automation tools are available for entities of all sizes and complexity. Selection of the appropriate compliance automation tool requires an entity to understand its regulatory environment, the risks it faces, and the maturity levels of its own compliance staff.
Relevant Threats and Vulnerabilities	• Non-compliance with management requirements • Inaccurate identification of managerial requirements • Unawareness of management requirements

M5.3.1	Compliance with Security Policies and Standards	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity's managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.					
Sub-Control	Managers shall: 1) identify all security procedures that fall within their area of responsibility 2) develop the capability to monitor the execution of identified security procedures 3) take corrective action when issues regarding the execution of security procedures are identified					

Implementation Guidance (for information purpose only)

Managers should regularly review the compliance of information processing within their area of responsibility with the appropriate security policies, standards, and any other security requirements.

If any non-compliance is found as a result of the review, managers should:

a. determine the causes of the non-compliance;
b. evaluate the need for actions to ensure that non-compliance do not recur;
c. determine and implement appropriate corrective action;
d. review the corrective action taken.

Results of reviews and corrective actions carried out by managers should be recorded and these records should be maintained. Managers should report the results to the persons carrying out the independent reviews, when the independent review takes place in the area of their responsibility

M5.4	Compliance with technical requirements
Objective	To ensure compliance of systems with technical security requirements
Performance Indicator	Percentage of information security technical sub-controls that have been implemented
Automation Guidance	Compliance automation tools are available for entities of all sizes and complexity. Selection of the appropriate compliance automation tool requires an entity to understand its regulatory environment, the risks it faces, and the maturity levels of its own compliance staff.
Relevant Threats and Vulnerabilities	• Non-compliance with technical requirements • Inaccurate identification of technical requirements • Unawareness of technical requirements

M5.4.1	Technical Compliance Checking	Priority / Applicability	P2 — Based on risk assessment
Control	The entity shall ensure that information systems are regularly checked for compliance with the UAE IA Regulation.		
Sub-Control	The entity shall: 1) define and execute a process for routinely checking for technical compliance with security standards 2) ensure results of compliance checking is performed by, and the results are reviewed by, authorized personnel with adequate technical capabilities 3) report any issues detected during technical compliance checking to the appropriate authority for remediation		

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard.

Technical compliance checking should be performed either manually (supported by appropriate software tools, if necessary) by an experienced system engineer, and/or with the assistance of automated tools, which generate a technical report for subsequent interpretation by a technical specialist.

If penetration tests or vulnerability assessments are used, caution should be exercised as such activities could lead to a compromise of the security of the system. Such tests should be planned, documented and repeatable.

Any technical compliance check should only be carried out by competent, authorized persons, or under the supervision of such persons.

M5.5	Information Systems Audit Considerations
Objective	To maximize the effectiveness of the information systems audit process taking into account TRA guidance in this regard
Performance Indicator	Percentage of audits interrupted due to operational or security issues
Automation Guidance	Compliance automation tools are available for entities of all sizes and complexity. Selection of the appropriate compliance automation tool requires an entity to understand its regulatory environment, the risks it faces, and the maturity levels of its own compliance staff.
Relevant Threats and Vulnerabilities	• Wrongly performed internal audit • Incorrect audit outcomes

M5.5.1	Information Systems Audit Controls	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity shall ensure that audit requirements and activities involving checks on operational systems are carefully planned and agreed to minimize the risk of disruptions to business processes.					
Sub-Control	The entity shall: 1) assign responsibilities for internal audits of information system controls to an appropriate authority 2) define audit requirements for information system controls 3) outline an audit plan to meet audit requirements for information system controls 4) highlight measures taken to ensure audit activities minimize the risk of disruptions to business processes					

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard.

The following guidelines should be observed:

a. audit requirements should be agreed with appropriate management;
b. the scope of the checks should be agreed and controlled;
c. the checks should be limited to read-only access to software and data;
d. access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements;
e. resources for performing the checks should be explicitly identified and made available;
f. requirements for special or additional processing should be identified and agreed;
g. all access should be monitored and logged to produce a reference trail; the use of time-stamped reference trails should be considered for critical data or systems;
h. all procedures, requirements, and responsibilities should be documented;
i. the person(s) carrying out the audit should be independent of the activities audited.

M5.5.2	Protection of Information Systems Audit Tools	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity shall protect access to information systems audit tools to prevent any possible misuse or compromise.					
Sub-Control	The entity shall: 1) identify all information systems audit tools 2) identify the types and classification levels of information stored in information systems audit tools 3) define minimum security requirements for information systems audit tools commensurate to the classification levels of the information held					
Implementation Guidance (for information purpose only)						

Information systems audit tools, e.g. software or data files, should be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection.

M5.5.3	Audit of Community Functions	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity shall specify the audit rights of members to the information sharing community to which it is connected to.					
Sub-Control	The entity shall: 1) identify the audit rights of any information sharing communities to which it is connected 2) ensure that provisions for external members are accounted for in the entity's information systems audit plan and tools 3) ensure that provisions for the entity to exercise its audit rights are accounted for in the entity's information systems audit plan and tools					
Implementation Guidance (for information purpose only)						

The authority to audit entity's systems could be limited to a trusted third party taking into account TRA guidance in this regard.

M6 Performance Evaluation and Improvement

M6	Performance Evaluation and Improvement
Objective	To ensure that information security performance is measured, analyzed, evaluated and improved, where necessary.
Performance Indicator	Compliance level achieved against the entity's information security policy and objectives (e.g. by using the performance indicators suggested in this Regulation or the entity's own performance indicators to produce a dashboard demonstrating compliance)

M6.1	Performance Evaluation Policy
Objective	To maintain a performance evaluation policy outlining the approach to measure and evaluate the effectiveness of the information security of the entity.
Performance Indicator	Percentage of successful performance measures applied
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• No performance evaluation • Performance evaluation against wrong criteria

M6.1.1	Performance Evaluation Policy	Priority	P3
		Applicability	Based on risk assessment
Control	The entity shall have a policy for performance evaluation that sets the framework for all performance evaluations that take place in the entity.		
Sub-Control	The entity shall develop and implement a performance evaluation policy that determines: 1) the overall framework for performance evaluation 2) the methods of reporting the performance evaluation results to management 3) how to integrate the detailed performance measurements for controls with higher level performance measurements for information security objectives, risk management, etc. 4) how to integrate incident reports in the overall picture of performance monitoring		

Implementation Guidance (for information purpose only)

Ongoing performance monitoring and evaluation is one of the major contributors to overall effective and success information security operation within any entity. Therefore, the entity should have an overall framework for its monitoring and performance measurement activities. These activities can have several sources of input:

a. high level performance evaluation activities, such as the performance indictors suggested for sub-families in this Regulation;
b. detailed performance evaluation activities, such as the performance indictors suggested for "risk-based applicable" controls;
c. ongoing monitoring, which detects deviations and necessary corrections;
d. incident reports, which indicate that one or more of the controls are not working as intended.

The performance evaluation policy should define how these different performance indicators are integrated within the entity to provide an overall picture of information security performance to management, and how the results of these performance measurement activities can be presented to management for decision-making.

M6.2	Performance Evaluation Policy
Objective	To ensure that information security performance is measured, analyzed and evaluated.
Performance Indicator	Percentage of all those con-conformities that have been detected and not resolved within the time frame planned
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Non-compliance with controls of this Regulation • Under-performance of information security controls in place • Ineffective controls

M6.2.1	Monitoring, Measurement, Analysis and Evaluation	Priority	P2
		Applicability	Always applicable
Control	The entity shall monitor and evaluate the information security performance and the effectiveness of the information security management system.		
Sub-Control	The entity shall: 1) determine: a. what needs to be monitored and measured, including information security processes and controls b. the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results c. when the monitoring and measuring shall be performed d. who shall monitor and measure e. when the results from monitoring and measurement shall be analyzed and evaluated f. who shall analyze and evaluate these results 2) document the monitoring and measurement methods and results.		

Implementation Guidance (for information purpose only)

The continual improvement the entity needs to apply to its information security controls (see also M6.3.2) needs to make use of the monitoring and performance measurement results to identify which areas do require improvement. Therefore, these activities are key to keeping information security up to date, and fit for purpose of the entity's requirements.

The results of monitoring and review should be recorded and externally and internally reported as appropriate, and should also be used as an input to the review of the information security risk management policy (refer to M2.1.1).

The entity should develop a plan to execute the monitoring and performance measurement activities, including all of the topics mentioned in the sub-controls above. It can be helpful to have clear responsibilities and schedule to carry out the monitoring and measuring, and there should be an independent review function that ensures that this monitoring takes place.

In addition to executing the monitoring and measurement activities, there is also a need to keep these activities up to date and effective, so all monitoring and performance evaluation activities should be subject periodical reviews, as well as immediate updates if the situation requires that.

The results of the monitoring and performance evaluation activities should be put into context with respect to

a. the information security policy (refer to M1.2.1)
b. the information security risk management policy (refer to M2.1.1)
c. management expectations with regards to information security and the overall internal context (refer to M1.1.1)
d. external requirements for information security, e.g. by the sector, regional or national

The methods selected for the monitoring and performance measurement should produce consistent and comparable results to assist the entity in measuring performance over time.

M6.2.2	Internal Audits	Priority	P2
		Applicability	Always applicable
Control	The entity shall plan and conduct internal audits of the information security in place.		
Sub-Control	The entity shall: 1) define the audit criteria, scope and audit plan for each audit 2) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process 3) ensure that the results of the audits are reported to relevant management 4) document the audit program and the audit results 5) ensure that the internal audit is effectively implemented and maintained The internal audits shall: 6) be planned, established, implemented and maintained, including the frequency, methods, responsibilities, planning requirements, and reporting of the internal audits 7) take account of the importance of the processes concerned and the results of previous audits 8) ensure that entity's information security conforms to: a. the entity's own requirements for information security b. the requirements of this Regulation c. any applicable requirements from the entity's sector, national or regulatory environment		

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard.

Internal audits are another important means, in addition to the performance measurements, to assess compliance with the "always applicable" controls of this Regulation, the entity's own policies and procedures, and the applicable requirements from the entity's sector, national or regulatory environment.

The information security controls in place at the entity should be subject to independent internal audits at a pre-defined schedule. This type of auditing should not come as a surprise but should be planned in advance, and the auditor should provide an audit plan of the areas to be audited and people to be met, to ensure the audit does not disrupt the business processes more than necessary (see also the sub-controls above).

One of the important concepts of internal audits is the independence of the internal auditor(s) carrying out the audits. If the necessary independence or expertise cannot be found within the entity, external resources can provide this service. If the entity uses external resources, care should be taken to ensure that the external resource have enough knowledge of the entity to successfully conduct the audit.
Another important aspect of the internal audit is the entity's reaction to its results. The results of the internal audits should be considered by the Information Security Committee (refer to M1.1.2), and it should be ensured that all findings of the audit are corrected in a timely manner.

M6.3	Improvement
Objective	To correct nonconformities with this Regulation and to continually improve the information security program in place
Performance Indicator	Number of all non-conformities that have been detected and not resolved within the time frame planned
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Non-compliance with the controls in this Regulation • Repeated incidents and inappropriate action to information security problems • No improvements to information security

M6.3.1	Corrective Action	Priority	P2
		Applicability	Always applicable
Control	The entity shall correct any nonconformity with these .		
Sub-Control	The entity shall react to the nonconformity when it occurs, and take action to control and correct it, and to deal with the consequences. The entity shall: 1) evaluate the need for action to eliminate the causes of nonconformities, in order that it does not recur or occur elsewhere, by: a. reviewing the nonconformity b. determining the causes of the nonconformity c. determining if similar nonconformities exist, or could potentially occur 2) implement the appropriate action needed to the effects of the encountered nonconformities 3) review the effectiveness of any corrective action taken 4) document the corrective actions taken against the nonconformities		

Implementation Guidance (for information purpose only)

The entity should have a clear action plan that describes how identified non-conformities will be addressed. This can take place in the Information Security Committee (refer to M1.1.2) and should be initiated and controlled by the Information Security Manager.

Determine whether corrective action is justified on the basis of evaluating the following considerations:

a. Whether it is a first or a repeat occurrence
b. Frequency and history of occurrences (repeated occurrences)
c. Seriousness of the impact
d. Root cause for the non-conformity for which the following activities have to be performed –
   - Collect data
   - Get expert advice
   - Consult with vendors, partners and associates

The corrective action(s) identified should be implemented within an appropriate timeframe and prioritized based on the risk treatment plan (see M2); delays should be avoided to reduce the negative effects of non-conformities to the information security in place at the entity.

It is also important to ensure that the implemented corrective actions achieve their intended objective and are effective. The review of the effectiveness of corrective actions can be done by the Information Security Committee, and the results should be documented.

M6.3.2	Continual Improvement	Priority	P2
		Applicability	Always applicable
Control	The entity shall continually improve the information security program in place.		
Sub-Control	The entity shall: 1) improve the suitability, adequacy and effectiveness of information security controls in place 2) take account of the performance measurement results and incidents when identifying improvements.		

Implementation Guidance (for information purpose only)

Based on results of monitoring and reviews, decisions should be made on how the information security in place, the controls, processes, policies and procedures can be improved. These decisions should lead to improvements in the entity's management of information security and its risk management culture.

Continual improvement of information security can be done through the entity's performance indicators and measurements, incident reports, training, reviews and audits (refer to M6.1) and the subsequent modification of the entity's processes, systems, resources, capability and skills.

Continual improvement is a very powerful concept and can help the entity to ensure that its information security is up to date and suitable for its needs.

5.4 Technical Controls

T1 Asset Management

T1	Asset Management
Objective	To ensure information classification and protection of organizational assets
Performance Indicator	Percentage of information assets that are adequately classified and protected

T1.1	Asset Management Policy
Objective	To maintain an asset management policy outlining the procedures to identify, classify and handle information assets
Performance Indicator	Extent of asset management policy deployment and adoption across the entity
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Use of unapproved hardware and / or devices • Physical theft of assets • Retrieval of recycled or discarded media

T1.1.1	Asset Management Policy	Priority		P2		
		Applicability	Based on risk assessment			
Control	The entity shall establish an asset management policy.					
Sub-Control	The asset management policy shall: 1) be appropriate to the complexity of the entity and to the assets managed by the entity 2) include statement of the management commitment, purpose, objective and scope of the policy 3) outline the roles and responsibilities 4) provide the framework for managing the entity's assets, including assignment of owners 5) provide the framework for managing Bring Your Own Device (BYOD) arrangements 6) be documented and communicated to all users 7) be read and acknowledged formally by all users 8) be maintained, reviewed and updated at planned intervals or if significant changes occur					

Implementation Guidance (for information purpose only)

The asset management policy provides a structure for the management of IT assets (e.g. people, hardware, software, data, facilities) from procurement to disposal. The policy can, for example, contain in addition to the required sub-controls:

a. IT Assets classification scheme
b. Classified assets security requirements
c. Disciplinary procedure

The asset management policy can be included as part of the general information security policy, in a single policy document, or can be represented by multiple policies reflecting the complex nature of certain entities.

T1.2	Responsibility for Assets
Objective	To achieve and maintain appropriate protection of the entity's information assets
Performance Indicator	Percentage of employees who have authorized access to information systems only after signing an acknowledgment of that they have read and understood rules of behavior
Automation Guidance	As a pre-requisite for any automation to be used, entities should identify assets and their owners, and then deciding and documenting which part of the entity and/or individuals are responsible for each component of a business process (including information, software, and hardware, IT, etc.). The entity could use a tool to automate the following processes: - tracking of information asset inventory, - assignment of information assets ownership - defining the right use of information assets Some entities maintain asset inventories using specific large-scale commercial products dedicated to the task, or they use free solutions to track and then sweep the network periodically for new assets connected to it. In particular, when entities acquire new systems, they record the owner and features of each new asset, including its network interface Media Access Control (MAC) address and location. This mapping of asset attributes and owner-to-MAC address can be stored in a free or commercial database management system. The entity should determine which asset attributes, based on entity's needs, should be tracked. The following list of potential attributes could be considered: - Asset name; - Asset type; - Asset tag; - IP address; - MAC address; - Serial number; - Location; etc.
Relevant Threats and Vulnerabilities	• Use of unapproved hardware and / or devices • Use of counterfeit or copied software • Destruction of Equipment or Media

T1.2.1	Inventory of Assets	Priority		P2		
		Applicability	Based on risk assessment			
Control	The entity shall maintain an inventory list of all its information assets.					
Sub-Control	The entity shall: 1) identify an inventory of information assets within the entity 2) maintain an up-to-date list of assets 3) ensure accuracy and consistency with other inventories					

Implementation Guidance (for information purpose only)

An entity should identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information should include creation, processing, storage, transmission, deletion, destruction, protection. Documentation should be done in dedicated or existing inventories as appropriate and includes asset data such as type of asset, location, backup information, related licenses, and its importance / criticality.

The asset inventory should be accurate, up to date, consistent, and aligned with other inventories such as inventories in Enterprise Asset Management and Enterprise Resource Planning (ERP).

Here is a list of inventory assets that might be considered including, but not limited to:

Hardware - Server

- Laptops, workstations, storage, security devices (firewall, IDS / IPS, anti-spam, etc.)

Network

- Routers, gateways, switches, Wireless Access Points, network segments (e.g. cabling and equipment between two computers), Others (SAT, Laser)

People

- Chief Technology / Information Director
- Information Technology Manager
- Database Development & Administration (manager, analyst, architect, administrator etc.)
- Programming / Software Engineering (manager, engineer, programmer, tester etc.) Back office Applications
- Financial control, customer care, logistics, ERP, CRM, Email

Client Facing Applications

- E-commerce, Internet Service Provisioning – Static, Public IP addresses, DNS services, Registration and management, Email service provisioning, and Web portals

Data and Information

- Customer personal data, customer financial data, entity's employee personal and financial data

Facilities

- Headquarters, secondary premises, branch offices, offices, and data centers

T1.2.2	Ownership of Assets	Priority			P2		
		Applicability	Based on risk assessment				
Control	The entity shall assign a designated owner for each asset in the inventory.						
Sub-Control	The entity shall: 1) establish the process for the assignment of asset ownership and its periodical review 2) assign an owner with management responsibility for each identified asset						

Implementation Guidance (for information purpose only)

The asset owner should be responsible for:
a. ensuring that information and assets associated with information systems are appropriately classified;
b. defining and periodically reviewing access restrictions and classifications, taking into account applicable access control policies.

Ownership may be allocated to:
- a business process;
- a defined set of activities;
- an application; or
- a defined set of data.

T1.2.3	Acceptable Use of Assets	Priority			P2		
		Applicability	Based on risk assessment				
Control	The entity shall develop rules for the acceptable use of its information assets.						
Sub-Control	The entity shall: 1) establish and document the rules for the acceptable use of assets 2) adapt rules to the different roles (management, users, administrators, operators, contractors, etc.) 3) ensure circulation and acceptance of the rules by employees, contractors and third parties 4) ensure compliance with the established rules						

Implementation Guidance (for information purpose only)

All employees, contractors and third party users should follow rules for the acceptable use of information and assets associated with information systems, including:
a. rules for electronic mail and Internet usages;
b. guidelines for the use of mobile devices, especially for the use outside the premises of the entity;
Specific rules or guidance should be provided by the relevant management. Employees, contractors and third party users using or having access to the entity's assets should be aware of the limits existing for their use of entity's information and assets associated with information systems, and resources. They should be responsible for their use of any information processing resources, and of any such use carried out under their responsibility.
Information provided by other members of an information sharing community is an asset, and should be protected and disseminated in accordance with any rules set by the information sharing community or by the originator.

T1.2.4	Acceptable Bring Your Own Device (BYOD) Arrangements	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall develop rules for the acceptable use of information assets associated with BYOD arrangements.		
Sub-Control	The entity shall: 1) establish the rules for the acceptable use of personal assets that are used on the entity's environment 2) adapt rules to the different roles (management, users, administrators, operators, contractors, etc.) 3) ensure circulation and acceptance of the rules by employees, contractors and third parties 4) measure compliance with these rules		

Implementation Guidance (for information purpose only)

All employees, contractors and third party users should follow rules for the acceptable use of information and assets associated with BYOD arrangements, including:

a. rules for phone, electronic mail and Internet usages;
b. rules for protection of the device from unauthorized access (e.g. pin code);
c. rules for storing and / or encrypting personal and entity information;
d. clear separation of personal data and entity's data.

It is recommended to ensure a complete split of personal and entity information by technical means.

T1.3	Information Classification
Objective	To ensure that information receives an appropriate level of protection
Performance Indicator	Percentage of information assets that are classification based on it sensitivity, versus those that are not
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Tampering with sensitive information with no appropriate protection • Unauthorized access to sensitive information

T1.3.1	Classification of Information	Priority			P3	
		Applicability			Based on risk assessment	
Control	The entity shall develop a classification scheme for its information.					
Sub-Control	The classification shall include: 1) an information classification scheme based on information value, legal requirements, sensitivity, and criticality to the entity 2) the degree of protection required for each category The information classification scheme shall ensure: 1) information classification based on the established levels and mapped to accountable owners 2) an up-to-date information classification in accordance with changes of their value, sensitivity and criticality through their life-cycle 3) the possibility to be accessed by automated systems to enforce specific protections based on the classification level 4) sufficient information regarding physical assets (locations, data centers, networks, systems, storage, etc.) used to store, process or transmit information assets is provided					

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard.

Classification and associated protective controls for information should take account of business needs for sharing or restricting information, as well as legal requirements. Assets other than information can also be classified in conformance with classification of information which is stored in, processed by or otherwise handled or protected by the asset.

A classification scheme should include conventions for classification and criteria for review of the classification over time; in accordance with some predetermined access control policy. The level of protection in the scheme should be assessed by analyzing confidentiality, integrity and availability and any other requirements for the information considered.

Owners of information assets should be accountable for their classification. The scheme should be consistent across the whole entity so that everyone will classify information and related assets in the same way, have a common understanding of protection requirements and apply the appropriate protection. Each level should be given a name that makes sense in the context of the classification scheme's application. Classification should be included in the entity's processes, and consistent and coherent across the entity. Results of classification should indicate value of assets depending on their sensitivity and criticality to the entity, e.g. in terms of confidentiality, integrity and availability. Results of classification should be updated in accordance with changes of their value, sensitivity and criticality through their life-cycle.

Classification provides people who deal with information a concise indication of how to handle and protect it. Creating groups of information with similar protection needs and specifying information security procedures that apply to all the information in the group facilitate this. This approach reduces the need for case-by-case risk assessment and custom design of controls.

An example of information confidentiality classification scheme could be based on four levels as follows:

a) disclosure causes no harm;
b) disclosure causes minor embarrassment or minor operational inconvenience;
c) disclosure has a significant short term impact on operations or tactical objectives;
d) disclosure has a serious impact on long term strategic objectives or put the survival of the organization at risk.

T1.3.2	Labeling of Information	Priority			P3	
		Applicability	Based on risk assessment			
Control	The entity shall label information in accordance with the classification scheme adopted by the entity.					
Sub-Control	The entity shall: 1) establish a procedure for labeling of information and its related assets in physical or electronic formats to reflect their attributed classification 2) apply the appropriate label on information					
Implementation Guidance (for information purpose only)						

Procedures for information labeling need to cover information and its related assets in physical and electronic formats. The labeling should reflect the classification scheme established in. The labels should be easily recognizable. The procedures should give guidance where and how labels are attached in consideration of how the information is accessed or the assets are handled depending on the types of media. The procedures can define cases where labeling is omitted, e.g. labeling of non-confidential information to reduce workloads. Employees and external party users should be made aware of labeling procedures.

Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label in the output.

T1.3.3	Handling of Information Assets	Priority			P3	
		Applicability	Based on risk assessment			
Control	The entity shall handle assets in accordance with the information classification scheme adopted by the entity.					
Sub-Control	The entity shall: 1) develop handling procedures for processing, storing and communicating information consistent with its classification and its attached label 2) safeguard the information in accordance with the established procedures					

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard.

Procedures should be drawn up for handling, processing, storing and communicating information consistent with its classification. The following items should be considered.

a. handling of all media to its indicated classification level of the information stored on it;
b. access restrictions to prevent access from unauthorized personnel;
c. maintenance of a formal record of the authorized recipients of assets;
d. protection of temporary or permanent copies of information to a level consistent with the protection of the original information; storage of IT assets in accordance with manufacturers' specifications;
e. keeping the distribution of assets to a minimum required to support the entity's needs;
f. clear marking of all copies of media for the attention of the authorized recipient.

The classification scheme used within the entity may not be equivalent to the schemes used by other entities, even if the names for levels are similar; in addition, information moving between entities may vary in classification depending on its context in each entity, even if their classification schemes are identical.

Agreements with other entities that include information sharing should include procedures to identify the classification of that information and to interpret the classification labels from other entities.

T1.4	Media Handling
Objective	To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities
Performance Indicator	Percentage of physical backup/archive media that are fully encrypted
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Destruction of equipment or media • Exploitation of backdoor or command and control channels • Retrieval of recycled or discarded media

T1.4.1	Management of Removable Media	Priority	P1
		Applicability	Based on risk assessment
Control	The entity shall manage the removable media in accordance with the classification scheme adopted by the entity.		
Sub-Control	The entity shall: 1) establish media management procedures along its lifecycle (setup, distribution, utilization and disposal) 2) identify the needed protection levels in accordance with the classification scheme 3) inhibit the use of removable media in those information systems that do not require it 4) control users of removable media		

Implementation Guidance (for information purpose only)

Removable media such as optical discs (Blu-ray discs, DVDs, CDs), memory cards (CompactFlash card, Secure Digital card, Memory Stick), floppy disks / zip disks, disk packs, and magnetic tapes, are typically found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices.

The following guidelines for the management of removable media should be considered:

a. if no longer required, the contents of any re-usable media that are to be removed from the entity should be made unrecoverable; data wiping software could be used for instance.
b. where necessary and practical, authorization should be required for media removed from the entity and a record of such removals should be kept in order to maintain an audit trail;
c. all media should be stored in a safe, secure environment, in accordance with manufacturers' specifications;
d. if data confidentiality or integrity are important considerations, cryptographic techniques should be used to protect data on removable media;
e. to mitigate the risk of media degrading while stored data are still needed, the data should be transferred to fresh media before it gets unreadable;
f. multiple copies of valuable data should be stored on separate media to further reduce the risk of coincident data damage or loss;
g. registration of removable media should be considered to limit the opportunity for data loss;
h. prevent content auto-run on laptops, workstations, and servers for removable media;
i. removable media drives should only be enabled if there is a business reason for doing so.

All procedures and authorization levels should be documented.

T1.4.2	Disposal of Media	Priority		P2		
		Applicability	Based on risk assessment			
Control	The entity shall dispose media when no longer needed.					
Sub-Control	The entity shall: 1) establish procedures for secure disposal of media containing confidential information based on the sensitivity of that information 2) destroy media, both paper and digital, when no longer serving the entity 3) keep records for disposed media (containing or used to contain confidential information) when no longer needed					

Implementation Guidance (for information purpose only)

Formal procedures for the secure disposal of media should be established to minimize the risk of confidential information leakage to unauthorized persons. The procedures for secure disposal of media containing confidential information should be corresponding with the sensitivity of that information.

The following items should be considered:

a. media containing confidential information should be stored and disposed of securely and safely, e.g. by incineration or shredding, or erased of data for use by another application within the entity;
b. procedures should be in place to identify the items that might require secure disposal;
c. it may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the sensitive items;
d. many entities offer collection and disposal services for media; care should be taken in selecting a suitable external party with adequate controls and experience;
e. disposal of sensitive items should be logged where possible in order to maintain an audit trail.

When accumulating media for disposal, consideration should be given to the aggregation effect, which may cause a large quantity of non-confidential information to become sensitive.

T2 Physical and Environmental Security

T2	Physical and Environmental Security
Objective	To prevent unauthorized physical access to the entity's facilities and ensure security of information and equipment
Performance Indicator	Frequency of information security breaches related to physical and environmental security

T2.1	Physical and Environmental Security Policy
Objective	To maintain a physical and environmental security policy to outline the security requirements of physical areas and equipment
Performance Indicator	Extent of physical and environmental security policy deployment and adoption across the entity
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Unsuitable environmental security policy • Unawareness of environmental security policy among staff • Wrong classification of secure areas

T2.1.1	Physical and Environmental Security Policy	Priority	P4
		Applicability	Based on risk assessment
Control	The entity shall develop and maintain a physical and environmental security policy to ensure appropriate physical protection of assets.		
Sub-Control	The physical and environmental security policy shall: 1) be appropriate to the purpose of the entity 2) include statement of the management commitment, purpose, objective and scope of the policy 3) outline the roles and responsibilities for the physical and environmental security 4) consider the Information Assets classification and their physical location (storage, processing, transfer) 5) be documented and communicated to all users 6) be read and acknowledged formally by all users 7) be maintained, reviewed and updated at planned intervals or if significant changes occur		

Implementation Guidance (for information purpose only)

The entity should develop, document, and disseminate the following documents to defined personnel or roles:

a. A physical and environmental security policy that addresses the purpose, scope, roles, responsibilities, management commitment, coordination to achieve appropriate physical protection among organizational entities, and compliance; and
b. Procedures to facilitate the implementation of the physical and environmental security policy and associated physical and environmental protection controls.

The entity should ensure that the physical and environmental security policy and all supporting procedures are periodically reviewed and updated.

T2.2	Secure Areas
Objective	To prevent unauthorized physical access, damage, and interference to the entity's premises and information
Performance Indicator	Percentage of resolved / closed corrective items identified from periodic physical security site surveys
Automation Guidance	Automated physical access management applications are available for entities of all sizes and complexity and are deployed along physical access control equipment (such as automated gates and doors). Selection of the appropriate access management application requires an entity to have an understanding of its physical landscape and locations, the risks it faces, and the protection level required.
Relevant Threats and Vulnerabilities	• Under protected secure areas • Unauthorized access to secure areas • Destruction of equipment of media • Interference with security controls

T2.2.1	Physical Security Perimeter	Priority		P2		
		Applicability	Based on risk assessment			
Control	The entity shall use security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) to protect areas that contain information and information systems.					
Sub-Control	The entity shall: 1) identify and classify security areas based on the assets and information they process or contain 2) define security perimeters for every classified security level to ensure the right level of protection is applied 3) ensure the right security countermeasures are adopted to protect areas that contain information and information systems					

Implementation Guidance (for information purpose only)

The following guidelines should be considered and implemented where appropriate for physical security perimeters:

a. security perimeters should be clearly defined, and the siting and strength of each of the perimeters should depend on the security requirements of the assets within the perimeter and the results of a risk assessment;
b. perimeters of a building or site containing information systems should be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur); the external walls of the site should be of solid construction and all external doors should be suitably protected against unauthorized access with control mechanisms, e.g. bars, alarms, locks etc.; doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level;
c. a manned reception area or other means to control physical access to the site or building should be in place; access to sites and buildings should be restricted to authorized personnel only;
d. physical barriers should, where applicable, be built to prevent unauthorized physical access and environmental contamination;
e. all fire doors on a security perimeter should be alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance to suitable regional, national, and international standards; they should operate in accordance with local fire code in a failsafe manner;
f. suitable intruder detection systems should be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas should be alarmed at all times; cover should also be provided for other areas, e.g. computer room or communications rooms;
g. information systems managed by the entity should be physically separated from those managed by third parties.

T2.2.2	Physical Entry Controls	Priority		P2		
		Applicability	Based on risk assessment			
Control	The entity shall protect secure areas by appropriate entry controls to ensure that only authorized personnel are allowed access.					
Sub-Control	The entity shall: 1) authenticate all persons accessing secure areas 2) document the access to secure areas 3) ensure that all persons wear some form of visible identification within the entity's premises 4) update and monitor access logs 5) in case of contractors/third parties, they shall be always escorted, unless the area is explicitly designated for them with no escort requirement					

Implementation Guidance (for information purpose only)

The following guidelines should be considered:

a. the date and time of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved; they should only be granted access for specific, authorized purposes and should be issued with instructions on the security requirements of the area and on emergency procedures.
b. access to areas where sensitive information is processed or stored should be controlled and restricted to authorized persons only; authentication controls, e.g. access control card plus PIN, should be used to authorize and validate all access; an audit trail of all access should be securely maintained;
c. all employees, contractors and third party users and all visitors should be required to wear some form of visible identification and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;
d. third party support service personnel should be granted restricted access to secure areas or sensitive information systems only when required; this access should be authorized and monitored;
e. access rights to secure areas should be regularly reviewed and updated, and revoked when necessary.

T2.2.3	Securing Offices, Rooms and Facilities	Priority / Applicability	P2 / Based on risk assessment
Control	The entity shall design and apply physical security for offices, rooms, and facilities.		
Sub-Control	The entity shall: 1) establish rules to avoid access by the public to key facilities in line with the physical and environmental policy 2) avoid obvious signs that indicates the type of information or activities in the secure areas		

Implementation Guidance (for information purpose only)

The following guidelines should be considered to secure offices, rooms, and facilities:

a. account should be taken of relevant health and safety and standards;
b. key facilities should be sited to avoid access by the public;
c. where applicable, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities;
d. directories and internal telephone books identifying locations of sensitive information systems should not be readily accessible by the public

T2.2.4	Protecting Against External and Environmental Threats	Priority / Applicability	P4 / Based on risk assessment
Control	The entity shall design and apply physical protection against natural disasters, malicious attack or accidents.		
Sub-Control	The entity shall: 1) establish policies and procedures for the storage of hazardous or combustible materials to reduce their risks on secure areas in line with the physical and environmental policy 2) secure fallback equipment and backup media from damage caused by a natural or man-made disaster 3) ensure that all physical protection countermeasures and procedures are aligned and coherent to Risk Assessment		

Implementation Guidance (for information purpose only)

Consideration should be given to any security threats presented by neighboring premises, e.g. a fire in a neighboring building, water leaking from the roof or in floors below ground level or an explosion in the street.

The following guidelines should be considered to avoid damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster:

a. hazardous or combustible materials should be stored at a safe distance from a secure area. Bulk supplies such as stationery should not be stored within a secure area;
b. fallback equipment and backup media should be sited at a safe distance to avoid damage from a disaster affecting the main site;
c. appropriate firefighting equipment should be provided and suitably placed.

T2.2.5	Working in Secure Areas	Priority / Applicability	P3 — Based on risk assessment
Control	The entity shall design physical protection and guidelines for working in secure areas.		
Sub-Control	The entity shall: 1) establish guidelines for working in secure areas 2) make sure all personnel accessing secure areas is aware and accepts rules and guidelines 3) supervise activities in secure areas 4) control access of devices to secure areas (See also T5.7.1)		

Implementation Guidance (for information purpose only)

The following guidelines should be considered:

a. personnel should only be aware of the existence of, or activities within, a secure area on a need to know basis;
b. unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities;
c. vacant secure areas should be physically locked and periodically checked;
d. photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorized;

The arrangements for working in secure areas include controls for the employees, contractors and third party users working in the secure area, as well as other third party activities taking place there

T2.2.6	Public Access, Delivery, and Loading Areas	Priority / Applicability	P3 — Based on risk assessment
Control	The entity shall control access points such as delivery and loading areas and other points.		
Sub-Control	The entity shall: 1) establish access procedures to loading and unloading areas to restrict access to only authorized personnel 2) physically segregate loading and unloading activities 3) inspect and register incoming and outgoing material in accordance with the entity's asset management procedures		

Implementation Guidance (for information purpose only)

The following guidelines should be considered:

a. access to a delivery and loading area from outside of the building should be restricted to identified and authorized personnel;
b. the delivery and loading area should be designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building;
c. the external doors of a delivery and loading area should be secured when the internal doors are opened;
d. incoming material should be inspected for potential threats before this material is moved from the delivery and loading area to the point of use;
e. incoming material should be registered in accordance with asset management procedures on entry to the site;
f. incoming and outgoing shipments should be physically segregated, where possible

T2.3	Equipment Security
Objective	To prevent loss, damage, theft or compromise of assets and interruption to the entity's activities
Performance Indicator	Percentage of performed checks that revealed unauthorized movement of information assets or other information security related issues
Automation Guidance	Solutions as physical access control, video surveillance and anti-intrusion systems should be considered.
Relevant Threats and Vulnerabilities	• Equipment failure • Tampering with equipment • Physical theft of asset

T2.3.1	Equipment Siting and Protection	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall site and protect equipment.		
Sub-Control	The entity shall: 1) establish guidelines for the physical protection of equipment against unauthorized access 2) monitor the environmental conditions and alert in case of a potential threat		

Implementation Guidance (for information purpose only)

The following guidelines should be considered to protect equipment:

a. equipment should be sited to minimize unnecessary access into work areas;
b. information systems handling sensitive data should be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use;
c. storage facilities should be secured to avoid unauthorized access;
d. items requiring special protection should be safeguarded to reduce the general level of protection required;
e. controls should be adopted to minimize the risk of potential physical and environmental threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism;
f. guidelines for eating, drinking and smoking in proximity to information systems should be established;
g. environmental conditions, such as temperature and humidity, should be monitored for conditions, which could adversely affect the operation of information systems;
h. lightning protection should be applied to all buildings and lightning protection filters should be fitted to all incoming power and communications lines;
i. the use of special protection methods, such as keyboard membranes, should be considered for equipment in industrial environments;
j. equipment processing confidential information should be protected to minimize the risk of information leakage due to electromagnetic emanation.

T2.3.2	Supporting Utilities	Priority / Applicability	P4 / Based on risk assessment
Control	The entity shall protect equipment from disruptions caused by failures in supporting utilities.		
Sub-Control	Supporting utilities shall: 1) be tested for any malfunctioning 2) ensure protection and uninterrupted power supply on information systems 3) provide emergency lighting in case of main power failure 4) have up-to-date utilities maintenance logs		

Implementation Guidance (for information purpose only)

Supporting utilities (e.g., electricity, telecommunications, water supply, natural gas, sewage, heating ventilation and air conditioning- should:

a. conform to equipment manufacturer's specifications and local legal requirements;
b. be appraised regularly for their capacity to meet business growth and interactions with other supporting utilities;
c. be inspected and tested regularly to ensure their proper functioning;
d. if necessary, be alarmed to detect malfunctions;
e. if necessary, have multiple feeds with diverse physical routing.

Emergency lighting and communications should be provided. Emergency switches and valves to cut off power, water, natural gas or other utilities should be located near emergency exits and/or equipment rooms.

T2.3.3	Cabling Security	Priority / Applicability	P4 / Based on risk assessment
Control	The entity shall protect power and telecommunication cabling carrying data or supporting information services.		
Sub-Control	The entity shall: 1) protect power and telecommunication cables against physical tempering 2) segregated power and telecommunication cables to prevent interference 3) scan the network on a regular basis to identify unauthorized devices connected to the network (refer to T5.4.3)		

Implementation Guidance (for information purpose only)

The following guidelines for cabling security should be considered:

a. power and telecommunications lines into information systems should be underground, where possible, or subject to adequate alternative protection;
b. power cables should be segregated from communications cables to prevent interference;
c. for sensitive or critical systems further controls to consider include:

1- installation of armored conduit and locked rooms or boxes at inspection and termination points;
2- use of electromagnetic shielding to protect the cables;
3- initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables;
4- controlled access to patch panels and cable rooms.

T2.3.4	Equipment Maintenance	Priority Applicability	P3 Based on risk assessment
Control	The entity shall maintain its equipment.		
Sub-Control	The entity shall: 1) document suppliers recommendations for the maintenance of equipment and make them available to maintenance personnel 2) establish policies and procedures for decommissioning and commissioning of equipment to ensure protection of sensitive data 3) keep maintenance logs for all equipment		

Implementation Guidance (for information purpose only)

The following guidelines for equipment maintenance should be considered:

a. equipment should be maintained in accordance with the supplier's recommended service intervals and specifications;
b. only authorized maintenance personnel should carry out repairs and service equipment;
c. records should be kept of all suspected or actual faults, and of all preventive and corrective maintenance;
d. appropriate controls should be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the entity; where necessary, confidential information should be cleared from the equipment or the maintenance personnel should be sufficiently cleared;
e. all maintenance requirements imposed by insurance policies should be complied with;
f. before putting equipment back into operation after its maintenance ensure that the equipment has not been tampered with and/or does not malfunction.

T2.3.5	Security of Equipment Off-Premises	Priority Applicability	P3 Based on risk assessment
Control	The entity shall apply security to off-site equipment.		
Sub-Control	The entity shall: 1) establish policies to protect off-site equipment in line with the physical and environmental policy (refer to M2.1.1)		

Implementation Guidance (for information purpose only)

The use of any information storing and processing equipment outside the entity's premises should be authorized by management. This applies to equipment owned by the entity and those owned privately and used on behalf of the entity.

The following guidelines should be considered for the protection of off-site equipment:

a. equipment and media taken off the premises should not be left unattended in public places; portable computers should be carried as hand luggage and disguised where possible when travelling;
b. manufacturers' instructions for protecting equipment should be observed at all times, e.g. protection against exposure to strong electromagnetic fields;

c. controls for off-premise locations, such as home-working, teleworking and temporary sites should be determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, access controls for computers and secure communication with the office;
d. it may be appropriate to avoid the risk by discouraging certain employees from working off-site and/or by restricting their use of portable IT equipment;
e. when off-premises equipment is transferred among different individuals or external parties, a log should be maintained that defines the chain of custody for the equipment including at least names and entities of those who are responsible for the equipment.

Risks, e.g. of damage, theft or eavesdropping, may vary considerably between locations and should be taken into account in determining the most appropriate controls.

T2.3.6	Secure Disposal or Re-Use of Equipment	Priority / Applicability	P3 / Based on risk assessment
Control	The entity shall ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.		
Sub-Control	The entity shall: 1) establish procedures for secure disposal or re-use of equipment based on the sensitivity of stored information 2) keep record of disposed equipment when no longer needed		
Implementation Guidance (for information purpose only)			

Equipment should be verified to ensure whether storage media is contained or not prior to disposal or re-use.
Storage media containing confidential information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using these delete or format function.

T2.3.7	Removal of Property	Priority / Applicability	P3 / Based on risk assessment
Control	The entity shall authorize any equipment, information or software that need to be taken off-site.		
Sub-Control	The entity shall: 1) establish an authorization procedure for taking information assets off-site 2) maintain the list of information assets off-site with the authorized employees, contractors and third party users		
Implementation Guidance (for information purpose only)			

The following guidelines should be considered:
a. equipment, information or software should not be taken off-site without prior authorization;
b. employees, contractors and third party users who have authority to permit off-site removal of assets should be clearly identified;
c. time limits for equipment removal should be set and returns checked for compliance;
d. where necessary and appropriate, equipment should be recorded as being removed off-site and recorded when returned

T2.3.8	Unattended User Equipment	Priority / Applicability	P2 / Based on risk assessment
Control	The entity shall ensure that unattended equipment has appropriate protection.		
Sub-Control	The entity shall: 1) establish user responsibilities and procedures when leaving equipment unattended 2) configure equipment and systems to implement automatic protections when left unattended		

Implementation Guidance (for information purpose only)

All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users should be advised to:

a. terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;
b. log-off from applications or network services when no longer needed;
c. secure computers or mobile devices from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use.

T2.3.9	Clear Desk and Clear Screen Policy	Priority / Applicability	P3 / Based on risk assessment
Control	The entity shall adopt a clear desk policy for papers and removable storage media and a clear screen policy.		
Sub-Control	The clear desk and clear screen policy shall: 1) be appropriate to the purpose of the entity 2) outline the responsibilities of the users with respect to clear desk and clear screen 3) be formalized and readily available to all users 4) be printed and made available to all desks subject to clear desk policy		

Implementation Guidance (for information purpose only)

The clear desk and clear screen policy should take into account the information classifications, legal and contractual requirements and the corresponding risks and cultural aspects of the entity. The following guidelines should be considered:

a. sensitive or critical business information (e.g. on paper, flipcharts, white boards or on electronic storage media), should be locked away ideally in a safe or cabinet or other forms of security furniture when not required, especially when the office is vacated.
b. computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use;
c. unauthorized use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) should be prevented;
d. media containing sensitive or classified information should be removed from printers immediately.

T3 Operations Management

T3	Operations Management
Objective	To ensure the effective operational control of the security functions related to information and information systems
Performance Indicator	Frequency of operational failures leading to information security incidents

T3.1	Operations Management Policy
Objective	To maintain an operations management policy and to provide guidance regarding the operational requirements of information assets
Performance Indicator	Extent of operations management security policy deployment and adoption across the entity
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Unsuitable operations management policy • Unawareness of operations management policy among staff

T3.1.1	Operations Management Policy	Priority					P4
		Applicability	Based on risk assessment				
Control	The entity shall establish an operations management policy.						
Sub-Control	The Operations Management Policy shall: 1) be appropriate to the purpose of the entity 2) provide the framework for managing the operations of systems, processes, and controls related to information security						

Implementation Guidance (for information purpose only)

The operations management policy defines and documents operational standards and procedures across the IT lifecycle (planning, design, implementation, operations, and maintenance) necessary to maximize information security. The policy can, for example, contain:

a. Scope of the policy
b. Segregation of duties
c. Configuration management
d. Change request
e. Quality management
f. Backup procedures
g. Monitoring procedures

The operations management policy can be included as part of the general information security policy, in a single policy document, or can be represented by multiple policies reflecting the complex nature of certain entities.

T3.2	Operational Procedures and Responsibilities
Objective	To ensure the correct and secure operation of information systems
Performance Indicator	Percentage of information systems that meet all operational information security requirements
Automation Guidance	Entities can implement control T3.2.1 by developing a series of images and secure storage servers for hosting these standard images. Commercial and/or free configuration management tools can then be employed to measure the settings operating system and applications of managed machines to look for deviations from these image configurations used by the entity. Some configuration management tools require that an agent be installed on each managed system, while others remotely log in to each managed machine using administrator credentials. Either approach or a combination of the two approaches can provide the information needed for this control.
Relevant Threats and Vulnerabilities	• Illegal processing of data • Abuse of system access/privileges • Equipment malfunction

T3.2.1	Common Systems Configuration Guidelines	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall develop recommended configuration settings for common information technology products.		
Sub-Control	The guidelines shall: 1) identify common information technology products used within the entity 2) define minimum security configurations to be employed in each product		

Implementation Guidance (for information purpose only)

Configuration settings guidelines for common information technology products should be created based on best practices and entity needs. These guidelines should be followed where applicable within the information system. Such products include operating systems (e.g., Microsoft Windows, Solaris) and databases (e.g., MS SQL, Oracle) and other products commonly used within the entity

T3.2.2	Documented Operating Procedures	Priority				P3	
		Applicability	Based on risk assessment				
Control	The entity shall document operating procedures.						
Sub-Control	The entity shall: 1) document operating procedures in a format that facilitates dissemination to all relevant stakeholders 2) ensure operating procedures are reviewed periodically 3) ensure all relevant stakeholders are aware of and have access to relevant operating procedures						

Implementation Guidance (for information purpose only)

Documented procedures should be prepared for system activities associated with information processing and communication systems, such as computer start-up and close-down procedures, back- up, equipment maintenance, media handling, computer room and mail handling management, and safety.

The operating procedures should specify the instructions for the detailed execution of each job including:

a. processing and handling of information;
b. backup;
c. scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;
d. instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities;
e. support contacts in the event of unexpected operational or technical difficulties;
f. special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs;
g. system restart and recovery procedures for use in the event of system failure;
h. the management of audit-trail and system log information.

Operating procedures, and the documented procedures for system activities, should be treated as formal documents and changes authorized by management. Where technically feasible, information systems should be managed consistently, using the same procedures, tools, and utilities

T3.2.3	Change Management	Priority					P4
		Applicability	Based on risk assessment				
Control	The entity shall control the changes to information systems.						
Sub-Control	The entity shall: 1) document a change management process 2) integrate specific process controls to ensure the change management process is executed correctly 3) define the systems to which the change management process applies 4) assign management responsibilities for control of changes to identified systems						

Implementation Guidance (for information purpose only)

Operational systems and application software should be subject to strict change management control. In particular, the following items should be considered:

a. identification and recording of significant changes;
b. planning and testing of changes;
c. assessment of the potential impacts, including security impacts, of such changes;
d. formal approval procedure for proposed changes;
e. communication of change details to all relevant persons;
f. fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.

Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures. When changes are made, an audit log containing all relevant information should be retained.

T3.2.4	Segregation of Duties	Priority		P2		
		Applicability	Based on risk assessment			
Control	The entity shall segregate duties and areas of responsibility.					
Sub-Control	The entity shall: 1) identify specific sets of duties that should be segregated 2) ensure duties with segregation requirements are assigned to different resources 3) implement suitable alternative controls in the case that duties with segregation requirements cannot be assigned to different resources					

Implementation Guidance (for information purpose only)

Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.

Small entities may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered. It is important that security audit remains independent

T3.2.5	Separation of Development, Test and Operational Facilities	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall separate development, test, and operational environment.		
Sub-Control	The entity shall: 1) identify the appropriate level of separation between operational, test, and development environments 2) define the rules for transferring software and systems from one environment to another 3) ensure the rules are integrated into the system / software development lifecycle		

Implementation Guidance (for information purpose only)

The level of separation between operational, test, and development environments that is necessary to prevent operational problems should be identified and appropriate controls implemented. The following items should be considered:

a. rules for the transfer of software from development to operational status should be defined and documented;
b. development and operational software should run on different systems or computer processors and in different domains or directories;
c. compilers, editors, and other development tools or system utilities should not be accessible from operational systems when not required;
d. the test system environment should emulate the operational system environment as closely as possible;
e. users should use different user profiles for operational and test systems, and menus should display appropriate identification messages to reduce the risk of error;
f. sensitive data should not be copied into the test system environment

T3.3	System Planning and Acceptance
Objective	To ensure security requirements are properly considered during the development lifecycle of information systems
Performance Indicator	Percentage of information systems that successfully integrated all system development lifecycle security requirements
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Equipment failure • Illegal processing of data • Use of counterfeit or copied software

T3.3.1	Capacity Management	Priority					P4
		Applicability	Based on risk assessment				
Control	The entity shall manage the required capacity.						
Sub-Control	The entity shall: 1) have the ability to measure capacity of current systems and estimate capacity requirements of planned systems 2) integrate capacity management controls into relevant demand management and software / system development lifecycle processes 3) make necessary adjustments to capacity to maintain required system performance						

Implementation Guidance (for information purpose only)

For each new and ongoing activity, capacity requirements should be identified. System tuning and monitoring should be applied to ensure and, where necessary, improve the availability and efficiency of systems. Detective controls should be put in place to indicate problems in due time. Projections of future capacity requirements should take account of new business and system requirements and current and projected trends in the entity's information processing capabilities.

Particular attention needs to be paid to any resources with long procurement lead times or high costs; therefore managers should monitor the utilization of key system resources. They should identify trends in usage, particularly in relation to business applications or management information system tools.

Managers should use this information to identify and avoid potential bottlenecks and dependence on key personnel that might present a threat to system security or services, and plan appropriate action.

T3.3.2	System Acceptance and Testing	Priority			P3	
		Applicability	Based on risk assessment			
Control	The entity shall establish acceptance criteria for new information systems, upgrades, and new versions, in addition to suitable tests of the system(s) carried out during development and prior to acceptance.					
Sub-Control	The entity shall: 1) define the requirements for testing new / updated systems prior to placing them in the operational environment 2) define the acceptable parameters for each requirement 3) ensure tests are carried out and that results are documented 4) formally assign responsibility for ensuring tests are completed prior to accepting new systems into operational environment					

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard.

Managers should ensure that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented, and tested. New information systems, upgrades, and new versions should only be migrated into production after obtaining formal acceptance. The following items should be considered prior to formal acceptance being provided:

a. performance and computer capacity requirements;
b. error recovery and restart procedures, and contingency plans;
c. preparation and testing of routine operating procedures to defined standards;
d. agreed set of security controls in place;
e. effective manual procedures;
f. business continuity arrangements;
g. evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times, such as month end;
h. evidence that consideration has been given to the effect the new system has on the overall security of the entity;
i. training in the operation or use of new systems;
j. ease of use, as this affects user performance and avoids human error.

For major new developments, the operations function and users should be consulted at all stages in the development process to ensure the operational efficiency of the proposed system design. Appropriate tests should be carried out to confirm that all acceptance criteria have been fully satisfied.

T3.4	Protection From Malware
Objective	To ensure that information and information systems are protected against malware.
Performance Indicator	Percentage of information systems with appropriate and up-to-date protection as defined in information security requirements.
Automation Guidance	Relying on policy and user action to keep anti-malware tools up to date has been widely discredited, as many users have not proven capable of consistently handling this task. To ensure anti-virus signatures are up to date, entities use automation. They use the built-in administrative features of enterprise endpoint security suites to verify that anti-virus, anti-spyware, and host-based IDS features are active on every managed system. They run automated assessments daily and review the results to find and mitigate systems that have deactivated such protections, as well as systems that do not have the latest malware definitions. Some entities deploy free or commercial honeypot and tarpit tools to identify attackers in their environment. Security personnel should continuously monitor honeypots and tarpits to determine whether traffic is directed to them and account logins are attempted. When they identify such events, these personnel should gather the source address from which this traffic originates and other details associated with the attack for follow-on investigation.
Relevant Threats and Vulnerabilities	• Spyware • Backdoor or command and control • SQL injection

T3.4.1	Controls Against Malware	Priority	P1
		Applicability	Based on risk assessment
Control	The entity shall protect its information assets from malware.		
Sub-Control	The entity shall: 1) employ anti-malware protection mechanisms for the network as well as servers, workstations, laptops and other devices connected to it 2) ensure that all anti-malware protection are up-to-date 3) periodically scan all information systems files as well as files downloaded from public networks 4) scan all email attachments before reaching user's inbox 5) scan removable media for malware every time they are connected to the information systems 6) configure servers, workstations, laptops so that they don't "auto-run" contents from removable media 7) monitor anti-malware protection tools for malware detection events that should be logged and a notification should be sent to the administrators (refer to T.3.6.2) 8) ensure that users are aware of malware risks, behaviors and preventative actions (refer to M.3.2.1)		

Implementation Guidance (for information purpose only)

Malware includes, for example, viruses, worms, Trojan horses, and spyware. Malware can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography.

Protection against malware should be based on malware detection and repair software, security awareness, and appropriate system access and change management controls. The following guidance should be considered:

a. establishing a formal policy prohibiting the use of unauthorized software;
b. establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures should be taken;
c. conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments should be formally investigated;
d. installation and regular update of software that detects and eradicate malware to scan computers and media as a precautionary control, or on a routine basis; the checks carried out should include:
   - reviewing any files received over networks or via any form of storage medium, for malware before use;
   - reviewing electronic mail attachments and downloads for malware before use; this check should be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the network of the entity;
   - checking web pages for malware;
e. defining management procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks;
f. preparing appropriate business continuity plans (refer to T9.2.2) for recovering from malware attacks, including all necessary data and software backup and recovery arrangements;
g. implementing procedures to regularly collect information, such as subscribing to mailing lists and/or checking web sites giving information about new malware;
h. implementing procedures to verify information relating to malware, and ensure that warning bulletins are accurate and informative; managers should ensure that qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malware, are used to differentiate between hoaxes and real malware; all users should be made aware of the problem of hoaxes and what to do on receipt of them;
i. isolate environments where catastrophic impacts may result.

Additional measures can include:

- monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality
- prevent content auto-run on laptops, workstations, and servers
- scan information systems periodically and files coming from external sources (including email attachments) in real-time
- periodically update the protection mechanism

T3.5	Backup
Objective	To maintain the integrity and availability of information and information systems.
Performance Indicator	Percentage of successful attempts to restore backup information, whether in test or real-world environments.
Automation Guidance	Commercial backup solutions are available to automatically perform information backup for designated systems. Entities deploying such solutions should carefully consider the following as examples: - what information should be covered during backup - when and at which frequency the backups should be conducted - where the backup data will be stored - what is the required total size of the medium to store the backups
Relevant Threats and Vulnerabilities	• Loss of information • Software malfunction • Destruction of equipment or media

T3.5.1	Information Backup	Priority	P1
		Applicability	Based on risk assessment
Control	The entity shall backup copies of its information and software.		
Sub-Control	The entity shall: 1) establish guidelines for determining what information and software requires backup and how often 2) establish and document clear backup procedures and system capabilities for all applicable backup requirements 3) ensure backed up information and software is routinely tested for reliability 4) ensure IT staff have the skills and qualification to conduct the backup procedures (refer to M1.4.1)		

Implementation Guidance (for information purpose only)

Adequate backup systems should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

The following items for information backup should be considered:

a. the necessary level of backup information should be defined;
b. accurate and complete records of the backup copies and documented restoration procedures should be produced;
c. the extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the entity, the security requirements of the information involved, and the criticality of the information to the continued operation of the entity;
d. - backups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site;
e. backup information should be given an appropriate level of physical and environmental protection consistent with these applied at the main site; the controls applied to media at the main site should be extended to cover the backup site;
f. backup media should be regularly tested to ensure that they can be relied upon for emergency use when necessary;
g. restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery;
h. in situations where confidentiality is of importance, backups should be protected by means of encryption.

Backup arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans (refer to T9.2.2). For critical systems, the backup arrangements should cover all systems information, applications, and data necessary to recover the complete system in the event of a disaster.

The retention period for essential business information, and also any requirement for archive copies to be permanently retained should be determined.

Once per quarter (or whenever new backup equipment is purchased), a testing team should evaluate a random sample of system backups by attempting to restore them on a test bed environment. The restored systems should be verified to ensure that the operating system, application, and data from the backup are all intact and functional.

T3.6	Monitoring
Objective	To detect, prevent and correct the use of systems and information based on audit logs of events that could impact the security of an entity.
Performance Indicator	Percentage of incidents within the entity where sufficient and accurate information was available to detect and manage the incident
Automation Guidance	Most free and commercial operating systems, network services, and firewall technologies offer logging capabilities. Such logging should be activated, with logs sent to centralized logging servers. Firewalls, proxies, and remote access systems (VPN, dial-up, etc.) should all be configured for verbose logging, storing all the information available for logging in the event a follow-up investigation is required. Furthermore, operating systems, especially those of servers, should be configured to create access control logs when a user attempts to access resources without the appropriate privileges. To evaluate whether such logging is in place, an entity should periodically scan through its logs and compare them with the asset inventory in order to ensure that each managed item actively connected to the network is periodically generating logs. Analytical programs such as SIM/SEM solutions for reviewing logs can provide value, but the capabilities employed to analyze audit logs are quite extensive, including, importantly, even just a cursory examination by a person. Actual correlation tools can make audit logs far more useful for subsequent manual inspection. Such tools can be quite helpful in identifying subtle attacks. However, these tools are neither a panacea nor a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition are often required to identify and understand attacks.
Relevant Threats and Vulnerabilities	• Unauthorized access • Tempering with information systems • Backdoor or command and control

T3.6.1	Monitoring Policy and Procedures	Priority			P3	
		Applicability	Based on risk assessment			
Control	The entity shall establish a monitoring policy and related procedures.					
Sub-Control	The monitoring policy and related procedures shall: 1) outline what system aspects shall be monitored, how they shall be monitored, and how often they shall be monitored 2) assign responsibility for monitoring activities 3) define how information from monitoring activities will be fed into the incident response process 4) account for any sector or national requirements regarding information to be shared with external entities 5) be documented					

Implementation Guidance (for information purpose only)

The entity should define events that need to be captured, the frequency of audit log reviews, and retention requirements for audit logs. Monitoring procedures should be developed, detailing the steps of the monitoring, the response actions and how the monitoring process feeds into the incident response process. Clear responsibilities should be assigned for the personnel performing monitoring. Each addition/ change of systems in the facility should be considered for the amendment of the monitoring policy and procedures, to ensure they properly cover the updated environment.

T3.6.2	Audit Logging	Priority		P2		
		Applicability	Based on risk assessment			
Control	The entity shall produce and keep audit logs recording user activities, exceptions, and information security events.					
Sub-Control	The entity shall: 1) identify all activities to be captured in audit logs for all hardware devices, operating systems and installed applications 2) identify minimum information requirements for each activity to be captured 3) define minimum frequency requirements for reviewing audit logs 4) ensure audit logs are reviewed by personnel with appropriate training and skills 5) define minimum time requirements for maintaining audit logs					

Implementation Guidance (for information purpose only)

Entities should log local and remote access (including failed attempts) to and from all hardware devices, operating systems and installed applications, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Audit logs should include, when relevant:

a. user IDs;
b. dates, times, and details of key events, e.g. log-on and log-off;
c. terminal identity or location if possible;
d. records of successful and rejected system access attempts;
e. records of successful and rejected data and other resource access attempts;
f. changes to system configuration;
g. use of privileges;
h. use of system utilities and applications;
i. files accessed and the kind of access;
j. network addresses and protocols;
k. alarms raised by the access control system;
l. activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems

T3.6.3	Monitoring System Use	Priority	P1
		Applicability	Based on risk assessment
Control	The entity shall monitor the use of information systems.		
Sub-Control	The entity shall: 1) identify all types of system use to be monitored 2) identify minimum information gathering requirements for each monitoring activity 3) define minimum frequency requirements for reviewing information gathered from monitoring activities 4) ensure information gathered from monitoring activities is reviewed by personnel with appropriate training and skills 5) define minimum time requirements for maintaining information gathered from monitoring activities		

Implementation Guidance (for information purpose only)

The level of monitoring required for individual systems should be determined by a risk assessment. An entity should comply with all relevant legal requirements applicable to its monitoring activities. Areas that should be considered include:

a. authorized access, including detail such as:
   1- the user ID;
   2- the date and time of key events;
   3- the types of events;
   4- the files accessed;
   5- the program/utilities used;

b. all privileged operations, such as:
   1- use of privileged accounts, e.g. supervisor, root, administrator;
   2- system start-up and stop;
   3- I/O device attachment/detachment;
   4- deleting, creating and granting privileges activities;

c. unauthorized access attempts, such as:
   1- failed or rejected user actions;
   2- failed or rejected actions involving data and other resources;
   3- access policy violations and notifications for network gateways and firewalls;
   4- alerts from proprietary intrusion detection systems;

d. system alerts or failures, such as:
   1- console alerts or messages;
   2- system log exceptions;
   3- network management alarms;
   4- alarms raised by the access control system;

e. database activities, such as:
   1- use of privileged accounts;
   2- backup / restore;
   3- failed or rejected user actions;

f. changes to, or attempts to change, system security settings and controls.

How often the results of monitoring activities are reviewed should depend on the risks involved. Risk factors that should be considered include the:

a. criticality of the application processes;
b. value, sensitivity, and criticality of the information involved;
c. past experience of system infiltration and misuse, and the frequency of vulnerabilities being exploited;
d. extent of system interconnection (particularly public networks);
e. logging facility being de-activated.

T3.6.4	Protection of Log Information	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall protect log information against tampering and unauthorized access.		
Sub-Control	The entity shall: 1) identify the log information across all information systems that shall be protected 2) ensure log information are protected commensurate to the sensitivity of the content of the logs		

Implementation Guidance (for information purpose only)

Controls should aim to protect against unauthorized changes and operational problems with the logging facility including:

a. alterations to the message types that are recorded;
b. log files being edited or deleted;
c. storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

Some audit logs may be required to be archived as part of the record retention policy or because of requirements to collect and retain evidence.

T3.6.5	Administrator and Operator Logs	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall log system administrator and system operator activities.		
Sub-Control	The entity shall: 1) identify all activities to be captured in administrator and operator logs 2) identify minimum information requirements for each activity to be captured 3) define minimum frequency requirements for reviewing administrator and operator logs 4) ensure administrator and operator logs are reviewed by personnel with appropriate training and skills 5) define minimum time requirements for maintaining administrator and operator logs		

Implementation Guidance (for information purpose only)

Logs should include:

a. the time at which an event (success or failure- occurred;
b. information about the event (e.g. files handled- or failure (e.g. error occurred and corrective action taken);
c. which account and which administrator or operator was involved;
d. which processes were involved.

System administrator and operator logs should be reviewed on a regular basis.

T3.6.6	Fault Logging	Priority			P3	
		Applicability	Based on risk assessment			
Control	The entity shall log faults related to information processing or communication					
Sub-Control	The entity shall: 1) identify all faults to be captured in fault logs 2) identify minimum information requirements for each fault to be captured 3) define minimum frequency requirements for reviewing fault logs 4) ensure fault logs are reviewed and analyzed by personnel with appropriate training and skills 5) define minimum time requirements for maintaining fault logs					

Implementation Guidance (for information purpose only)

Fault Logging enables systems to log and report faults (problems, errors or failures) related to information processing or communications. Faults reported by users or by system programs should be logged. There should be clear rules for handling reported faults including:

a. review of fault logs to ensure that faults have been satisfactorily resolved;
b. review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorized.

It should be ensured that error logging is enabled, if this system function is available.

T3.6.7	Clock Synchronization	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity shall synchronize clocks of all relevant information systems with an agreed accurate time source.					
Sub-Control	The entity shall: 1) define the date / time format and these standard time to be used in all systems 2) define the stratum level of clocks needed for each type of network element 3) regularly check that the clocks of all relevant information processing systems are synchronized					

Implementation Guidance (for information purpose only)

Where a computer or communications device has the capability to operate a real-time clock, this clock should be set to an agreed standard, e.g. Coordinated Universal Time (UTC- or local standard time. As some clocks are known to drift with time, there should be a procedure that checks for and corrects any significant variation.

The correct interpretation of the date/time format is important to ensure that the timestamp reflects the real date/time. Local specifics (e.g. daylight savings) should be taken into account.

T4 Communications

T4	Communications
Objective	To ensure the protection of information being exchanged within and between entities
Performance Indicator	Frequency of breaches of information during communications

T4.1	Communications Policy
Objective	To maintain a communications policy covering the security of information shared internally and externally
Performance Indicator	Extent of communications policy deployment and adoption across the entity
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Unsuitable communications policy • Unawareness of communications policy among IT staff

T4.1.1	Communications Policy	Priority			P3	
		Applicability	Based on risk assessment			
Control	The entity shall establish a communications policy to guide the protection of information in transit.					
Sub-Control	The communications policy shall: 1. be appropriate to the purpose of the entity 2. include statement of the management commitment, purpose, objective and scope of the policy 3. outline the roles and responsibilities 4. provide the framework to protect information in transit from interception, copying, modification, mis-routing, destruction, and other unauthorized activities 5. be documented and communicated to all users 6. be read and acknowledged formally by all users 7. be maintained, reviewed and updated at planned intervals or if significant changes occur					

Implementation Guidance (for information purpose only)

The communications policy facilitates the implementation of the associated controls to secure information in transit and information sharing. The policy can, for example, contain in addition to the required sub-controls:

a. Information transfer procedures
b. Physical media transfer procedures
c. Electronic messaging
d. Information sharing protection
e. Network security management

The communications policy can be included as part of the general information security policy, in a single policy document, or can be represented by multiple policies reflecting the complex nature of certain entities.

T4.2	Information Transfer
Objective	To maintain the security of information and software exchanged within an entity and with any external entity.
Performance Indicator	Percentage of people not complying with the information transfer policy.
Automation Guidance	Commercial DLP solutions are available to look for exfiltration attempts and detect other suspicious activities associated with a protected network holding sensitive information. Entities deploying such tools should carefully inspect their logs and follow up on any discovered attempts, even those that are successfully blocked, to transmit sensitive information out of the entity without authorization.
Relevant Threats and Vulnerabilities	• Unprotected information in transit • Tempering with information systems

T4.2.1	Information Transfer Procedures	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall develop formal transfer procedures and controls should be in place to protect the exchange of information.		
Sub-Control	The entity shall: 1) Establish information transfer procedures The procedures shall: 1) outline conditions under which the transfer of information must be protected 2) identify specific controls to be put in place to ensure information is adequately protected during transfer 3) identify actions to be taken when issues arise regarding the transfer of information 4) be documented, maintained, reviewed and updated at planned intervals or if significant changes occur		

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard.

The procedures and controls to be followed when using communication systems for information transfer should consider the following items:

a. procedures designed to protect transferred information from interception, copying, modification, mis-routing and destruction;
b. procedures for the detection of and protection against malware that may be transmitted through the use of electronic communications;
c. procedures for protecting communicated sensitive or confidential electronic information that is in the form of an attachment;
d. policy or guidelines outlining acceptable use of communication systems;
e. personnel, external party and any other user's responsibilities not to compromise the entity, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.;
f. use of cryptographic techniques e.g. to protect the confidentiality, integrity and authenticity of information;
g. retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant national and local legislation and ;
h. controls and restrictions associated with using communication systems, e.g. automatic forwarding of electronic mail to external mail addresses;
i. advise personnel to take appropriate precautions not to reveal sensitive or confidential information;
j. not leaving messages containing sensitive or confidential information on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialing;
k. advise personnel about the problems of using facsimile machines, namely:
1- unauthorized access to built-in message stores to retrieve messages;
2- deliberate or accidental programming of machines to send messages to specific numbers;
3- sending documents and messages to the wrong number either by misdialing or using the wrong stored number.

In addition, personnel should be reminded that they should not have confidential conversations in public places or over unsecure communication channels, open offices and meeting places. Information transfer services should comply with any relevant legal requirements.

T4.2.2	Agreements on Information Transfer	Priority			P3	
		Applicability	Based on risk assessment			
Control	The entity shall establish agreements for the exchange of information and software between the entity and external parties.					
Sub-Control	The entity shall: 1) identify all security requirements for exchanging information and software with external parties 2) establish an exchange of information agreement with each external party outlining clear roles and responsibilities of each party 3) ensure external parties are aware of all information security requirements and policies that are necessary before signing the agreement 4) monitor the exchange of information and software with external parties to ensure the requirements in the agreement are being met 5) take corrective action when the exchange of information or software does not follow the terms of the agreement					

Implementation Guidance (for information purpose only)

Exchange agreements should consider the following security conditions:

a. management responsibilities for controlling and notifying transmission, dispatch, and receipt;
b. procedures for notifying sender of transmission, dispatch, and receipt;
c. procedures to ensure traceability and non-repudiation;
d. minimum technical standards for packaging and transmission;
e. escrow agreements;
f. courier identification standards;
g. responsibilities and liabilities in the event of information security incidents, such as loss of data;
h. use of an agreed labeling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected;
i. ownership and responsibilities for data protection, copyright, software license compliance and similar considerations;
j. technical standards for recording and reading information and software;
k. any special controls that may be required to protect sensitive items, such as cryptographic keys.

Policies, procedures, and standards should be established and maintained to protect information and physical media in transit (refer to T4.2.3), and should be referenced in such exchange agreements.

The security content of any agreement should reflect the sensitivity of the business information involved.

T4.2.3	Physical Media in Transit	Priority				P3	
		Applicability	Based on risk assessment				
Control	The entity shall protect physical media containing information during transportation.						
Sub-Control	The entity shall: 1) identify physical media carrying sensitive information 2) define labeling requirements for physical media carrying sensitive information 3) ensure physical media in transit carrying sensitive information is tracked sufficiently in accordance with the sensitivity of the information it contains 4) define measures to be taken in the event of loss of physical media in transit carrying sensitive information 5) keep a log of all transitions						

Implementation Guidance (for information purpose only)

The following guidelines should be considered to protect media containing information being transported between sites:

a. reliable transport or couriers should be used;
b. a list of authorized couriers should be agreed with management;
c. procedures to verify the identification of couriers should be developed;
d. packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications (e.g. for software), for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields;
e. logs should be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and the receipt at destination.

T4.2.4	Electronic Messaging	Priority				P3	
		Applicability	Based on risk assessment				
Control	The entity shall protect information involved in electronic messaging.						
Sub-Control	The entity shall: 1) identify all means of electronic messaging in which the entity's information assets can be transmitted 2) for each category of electronic messaging identified, define rules regarding the type of information that can be transmitted and specific controls needed 3) develop the capability to monitor electronic messaging to ensure controls are implemented and the rules are followed 4) take corrective action when information is transmitted through electronic messaging in a manner inconsistent with the established rules						

Implementation Guidance (for information purpose only)

Security considerations for electronic messaging should include the following:

a. protecting messages from unauthorized access, modification or denial of service;
b. ensuring correct addressing and transportation of the message;
c. general reliability and availability of the service;
d. legal considerations, for example requirements for electronic signatures;
e. obtaining approval prior to using external public services such as instant messaging or file sharing;
f. stronger levels of authentication controlling access from publicly accessible networks.

T4.2.5	Business Information Systems	Priority					P4
		Applicability	Based on risk assessment				
Control	The entity shall develop policies and procedures to protect information transferred across business information systems.						
Sub-Control	The policies and procedures shall: 1) identify all points of interconnection between business information systems 2) identify the types of information to be protected regarding the identified interconnections 3) identify appropriate security measures to be taken to protect each type of information 4) be documented, maintained, reviewed and updated at planned intervals or if significant changes occur						

Implementation Guidance (for information purpose only)

Consideration given to the security and business implications of interconnecting such systems should include:

a. known vulnerabilities in the administrative and accounting systems where information is shared between different parts of the entity;
b. vulnerabilities of information in business communication systems, e.g. recording phone calls or conference calls, confidentiality of calls, storage of facsimiles, opening mail, distribution of mail;
c. policy and appropriate controls to manage information sharing;
d. excluding categories of sensitive business information and classified documents if the system does not provide an appropriate level of protection;
e. restricting access to diary information relating to selected individuals, e.g. personnel working on sensitive projects;
f. categories of personnel, contractors or business partners allowed to use the system and the locations from which it may be accessed;
g. restricting selected systems to specific categories of user;
h. identifying the status of users, e.g. employees of the entity or contractors in directories for the benefit of other users;
i. retention and backup of information held on the system;
j. fallback requirements and arrangements.

T4.3	Electronic Commerce Services
Objective	To ensure the security of electronic commerce services
Performance Indicator	Percentage of e-commerce volume subject to information security incidents
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Embezzlement, skimming, and related fraud • Eavesdropping / Packet Sniffing

T4.3.1	Electronic Commerce	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall protect information involved in electronic commerce passing over public networks from fraudulent activity, contract dispute, and unauthorized disclosure and modification.		
Sub-Control	The entity shall: 1) identify all instances of electronic commerce within the entity that require passing information over public networks 2) identify appropriate security measures for information passing over public networks based on the risk assessment 3) ensure security requirements are captured in service agreements with e-commerce partners 4) monitor e-commerce activities for on-going compliance with security requirements		

Implementation Guidance (for information purpose only)

Security considerations for electronic commerce should include the following:

a. the level of confidence each party requires in each other's claimed identity, e.g. through authentication;
b. authorization processes associated with who may set prices, issue or sign key trading documents;
c. ensuring that trading partners are fully informed of their authorizations;
d. determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents, and the non-repudiation of contracts, e.g. associated with tendering and contract processes;
e. the level of trust required in the integrity of advertised price lists;
f. the confidentiality of any sensitive data or information;
g. the confidentiality and integrity of any order transactions, payment information, delivery address details, and confirmation of receipts;
h. the degree of verification appropriate to check payment information supplied by a customer;
i. selecting the most appropriate settlement form of payment to guard against fraud;
j. the level of protection required to maintain the confidentiality and integrity of order information;
k. avoidance of loss or duplication of transaction information;
l. liability associated with any fraudulent transactions;
m. insurance requirements.

Many of the above considerations can be addressed by the application of cryptographic controls , taking into account compliance with legal requirements.

Electronic commerce arrangements between trading partners should be supported by a documented agreement which commits both parties to the agreed terms of trading, including details of authorization (see b- above). Other agreements with information service and value added network providers may be necessary.

Public trading systems should publicize their terms of business to customers. Consideration should be given to the resilience to attack of the host(s) used for electronic commerce, and the security implications of any network interconnection required for the implementation of electronic commerce services.

T4.3.2	On-Line Transactions	Priority	P3
		Applicability	Based on risk assessment
Control	The entity shall protect information involved in on-line transactions against incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.		
Sub-Control	The entity shall: 1) identify all information used in on-line transactions 2) identify appropriate security measures for information used in on-line transactions based on the risk assessment 3) ensure security requirements are captured in service agreements with all partners involved in on-line transactions 4) monitor on-line transactions for on-going compliance with security requirements		

Implementation Guidance (for information purpose only)

Security considerations for on-line transactions should include the following:

a. the use of electronic signatures by each of the parties involved in the transaction;
b. all aspects of the transaction, i.e. ensuring that:
1- user credentials of all parties are valid and verified;
2- the transaction remains confidential; and
3- privacy associated with all parties involved is retained;
c. communications path between all involved parties is encrypted;
d. protocols used to communicate between all involved parties is secured;
e. ensuring that the storage of the transaction details are located outside of any public accessible environment, e.g. on a storage platform existing on the organizational Intranet, and not retained and exposed on a storage medium directly accessible from the Internet;
f. where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures and/or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process

T4.3.3	Publicly Available Information	Priority / Applicability	P4 / Based on risk assessment
Control	The entity shall protect information being made available on a publicly available system against unauthorized modification.		
Sub-Control	The entity shall: 1) identify all information to be made available on a publicly available system 2) define security requirements for information to be made available on a publicly available system based on the risk assessment 3) monitor information being made available on publicly available systems for unauthorized modification 4) ensure that all public information is sanitized and approved		

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard.

Software, data, and other information requiring a high level of integrity, being made available on a publicly available system, should be protected by appropriate mechanisms, e.g. digital signatures. The publicly accessible system should be tested against weaknesses and failures prior to information being made available.

There should be a formal approval process before information is made publicly available. In addition, all input provided from the outside to the system should be verified and approved.

Electronic publishing systems, especially those that permit feedback and direct entering of information, should be carefully controlled so that:

a. information is obtained in compliance with any data protection legislation;
b. information input to, and processed by, the publishing system will be processed completely and accurately in a timely manner;
c. sensitive information will be protected during collection, processing, and storage;
d. access to the publishing system does not allow unintended access to networks to which the system is connected

T4.4	Information Sharing Protection
Objective	To ensure adequate protection of information shared within an information sharing community.
Performance Indicator	Frequency of information security incidents occurring within each information sharing community in which information is intentionally or unintentionally disclosed.
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Misappropriation of private knowledge • Abuse of system access/privileges

T4.4.1	Connectivity to Information Sharing Platforms	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity shall ensure that connectivity to information sharing platforms should be secured.					
Sub-Control	The entity shall: 1) identify all relevant information sharing platforms to which the entity will connect 2) determine the security requirements for connecting to identified platforms 3) identify specific controls needed to meet the security requirements for each information sharing platform 4) develop the capabilities needed for secure connectivity to any required sector, national, or international information sharing communities					

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard (also refer to National Cyber Information Sharing Policy).

While most information sharing communities are built on a voluntary basis, certain entities may also have mandatory requirements to join specific information sharing platforms (e.g. sector or national level platforms established by regulators or other national authorities).

In all cases, it is the responsibility of the information sharing platform manager to outline minimum security requirements for all information sharing community members. This helps install a basic component of trust that all community members have the minimum security controls in place to protect the information being shared on the platform.

Entities looking to connect to information sharing platforms should contact the platform manager for security requirements and ensure all requirements are fully understood and implemented.

T4.4.2	Information Released into Information Sharing Communities	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity shall follow the format, classification, and treatment requirements of the information sharing community for information released into information sharing communities.					
Sub-Control	For each connected information sharing platform, the entity shall: 1) identify all information to be released into the information sharing community utilizing the platform 2) implement minimum format, classification, and treatment requirements as outlined by the platform manager 3) identify and implement any additional security requirements needed to protect the released information in line with the entity's risk assessment 4) develop the capabilities needed to share information securely within any required sector, national or international information sharing communities					

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard (also refer to National Cyber Information Sharing Policy).

Based on urgency, potential consequences and technical constraints, it may not be possible for an entity to validate all information before transmission into the information sharing community. Where limitations exist, these should be indicated as part of the message. Also, indicating reservations on credibility of information is particularly important where the source is anonymous or unknown. It is important to indicate where the originator has been able to validate the information given directly, and can vouch for its authenticity.

There are technical mechanisms that can be used to provide authenticity without compromising anonymity. For example, shared cryptographic secrets could be used to confirm that a communication originated from a member of the community without revealing the actual identity of the originator. Each recipient should be responsible for obtaining any necessary authorizations for wider release from the originator prior to onwards distribution.

In inter-sector communications, the originator may not know who all the entities that receive the information will be. In such a case, a general or specific sector release approval will need to be granted. In addition, all information sharing communities should define rules for the protection of information in transit, and only permit members to join the community if such rules are accepted and implemented by the prospective member. Any supporting entity should implement such rules internally.

Information sharing communities should consider implementing alternative mechanisms for information sharing that do not rely on electronic messaging, and enabling members to specify that specific messages are distributed by such other routes.

T4.5	Network Security Management
Objective	To ensure the protection of information in networks and the protection of the supporting infrastructure.
Performance Indicator	Percentage of information systems that meet all network security management requirements.
Automation Guidance	Port scanning tools are used on a range of target systems to determine which services are listening on the network. In addition to determining which ports are open, effective port scanners can be configured to identify the version of the protocol and service listening on each discovered open port. This list of services and their versions are compared against an inventory of services required by the entity for each server and workstation in an asset management system. Recently added features in these port scanners are being used to determine the changes in services offered by scanned machines on the network since the previous scan, helping security personnel identify differences over time.
Relevant Threats and Vulnerabilities	• Abuse of system access/privileges • Eavesdropping / Packet Sniffing • Denial of Service (DOS) or DDOS

T4.5.1	Network Controls	Priority	P1
		Applicability	Based on risk assessment
Control	The entity shall ensure that all networks are adequately managed, controlled, and protected.		
Sub-Control	The entity shall: 1) identify all network components and interconnectivity between them 2) document and maintain network diagram that includes all network components as well as their connections 3) perform a risk assessment on individual network components and the network as a whole to identify vulnerabilities requiring action 4) identify and implement specific network controls needed to mitigate the vulnerabilities identified 5) continually monitor the in-place controls for efficiency and effectiveness		

Implementation Guidance (for information purpose only)

Network managers should implement controls to ensure the security of information in networks, and the protection of connected services from unauthorized access. In particular, the following items should be considered:

a. operational responsibility for networks should be separated from computer operations where appropriate;
b. responsibilities and procedures for the management of remote equipment, including equipment in user areas, should be established;
c. special controls may be required to maintain the availability of the network services and computers connected;
d. management activities should be closely coordinated both to optimize the service to the entity and to ensure that controls are consistently applied across the information processing infrastructure.

Further measures can include:

e. implement ingress and egress filtering to allow only those ports and protocols with an explicit and documented business need;
f. restrict access only to trusted sites (white lists);
g. inspect packets on DMZ networks using Security Event Information Management (SEIM) or log analytics systems;
h. deploy Sender Policy Framework (SPF) records in DNS and enabling receiver-side verification in mail servers;
i. disable / uninstall unused services;
j. enable host-based firewalls or port filtering tools on end systems with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed;
k. regularly scan port on all key servers, and compare results to a known effective baseline;
l. backup and protect firewall, router, and switch configurations.

T4.5.2	Security of Network Services	Priority / Applicability	P2 / Based on risk assessment
Control	The entity shall identify the security features, service levels, and management requirements of all network services and include these requirements in any network services agreement, whether these services are provided in-house or outsourced.		
Sub-Control	The entity shall: 1) specify which network services are subject to specific security requirements 2) define minimum security requirements for each identified service 3) ensure minimum security requirements are captured in service level agreements for network services 4) ensure minimum security requirements are implemented in network services		

Implementation Guidance (for information purpose only)

The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored, and the right to audit should be agreed.

The security arrangements necessary for particular services, such as security features, service levels, and management requirements, should be identified. The entity should ensure that network service providers implement these measures.

T4.5.3	Segregation in Networks	Priority / Applicability	P1 / Based on risk assessment
Control	The entity shall segregate groups of information services, users, and information systems on networks.		
Sub-Control	The entity shall: 1) identify criteria for grouping information services, users, and information systems into different groups that facilitate segregation on networks 2) for each group, identify specific segregation requirements 3) ensure identified segregation requirements are included in the relevant system / service development lifecycle 4) periodically evaluate the effectiveness of implemented segregation strategies and identify areas for improvement		

Implementation Guidance (for information purpose only)

One method of controlling the security of large networks is to divide them into separate logical network domains, e.g. an entity's internal network domains and external network domains, each protected by a defined security perimeter. A graduated set of controls can be applied in different logical network domains to further segregate the network security environments, e.g. publicly accessible systems, internal networks, and critical assets. The domains should be defined based on a risk assessment and the different security requirements within each of the domains.

Such a network perimeter can be implemented by installing a secure gateway between the two networks to be interconnected to control access and information flow between the two domains. This gateway should be configured to filter traffic between these domains and to block unauthorized access in accordance with the entity's access control policy. An example of this type of gateway is what is commonly referred to as a firewall. Another method of segregating separate logical domains is to restrict network access by using virtual private networks for user groups within the entity.

Networks can also be segregated using the network device functionality, e.g. IP switching. Separate domains can then be implemented by controlling the network data flows using the routing/switching capabilities, such as access control lists.

The criteria for segregation of networks into domains should be based on the access control policy and access requirements, and also take account of the relative cost and performance impact of incorporating suitable network routing or gateway technology.

In addition, segregation of networks should be based on the value and classification of information stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption.

T4.5.4	Security of Wireless Networks	Priority		P2		
		Applicability	Based on risk assessment			
Control	The entity shall ensure that all wireless networks are adequately secured.					
Sub-Control	The entity shall: 1) undertake and document a site survey to determine the optimal physical locations to avoid stray signal leaking too far outside of the entity's physical perimeter 2) identify criteria for grouping information services, users, and information systems into different groups that facilitate segregation on wireless networks 3) for each wireless network, identify the security controls that should be in place based on the required protection level of the information services, users, and information systems it supports 4) periodically evaluate the effectiveness of implemented segregation strategies and identify areas for improvement					

Implementation Guidance (for information purpose only)

Consideration should be given to the segregation of wireless networks from internal and private networks. As the perimeters of wireless networks are not well defined, a risk assessment should be carried out in such cases to identify controls (e.g. strong authentication, cryptographic methods, and frequency selection) to maintain network segregation.

When designing its wireless networks, the entity should consider the number of base stations to be deployed, where they will be situated, what bandwidth limitations should apply to clients and what wired alternatives should exist, so as to limit the potential for wireless-based Denial of Service attacks.
The use of 'guest' wireless networks should be restricted to genuine short-term guests of the Entity and consultants without a verified need for connection to the Entity's core network. Guest networks should only connect to the Internet and their data should not transit via the Entity's core network. Traffic on wireless guest networks should not be terminated on the core network and should be tunnelled directly to the network perimeter.

Traffic on guest networks should be monitored by the entity to ensure conformance with its acceptable usage provisions. Temporary users of guest networks should be required to authenticate to the network, to avoid opportunistic use of the Entity's network resources.

Network managers should implement controls to ensure the security of information in wireless. In particular, special controls should be established to safeguard the confidentiality and integrity of data passing over wireless networks, and to protect the connected systems and applications.

The entity should prohibit and sanction the creation and use of ad-hoc wireless networks, including the connecting of unapproved wireless base-stations to the entity's core data network.

The entity should put in place mechanisms that allow for the identification and isolation of rogue wireless access points.

T5 Access Control

T5	Access Control
Objective	To institute access control at the user, application, network and operating system level as well as for mobile computing.
Performance Indicator	Number of blocked attempts at unauthorized access

T5.1	Access Control Policy
Objective	To maintain an access control policy covering user authorization procedures to information assets
Performance Indicator	Extent of access control policy deployment and adoption across the entity
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Unsuitable access control policy • Unawareness of access control policy among IT staff

T5.1.1	Access Control Policy	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall establish an access control policy based on business and security requirements.		
Sub-Control	The access control policy shall: 1) be appropriate to the purpose of the entity 2) include statement of the management commitment, purpose, objective and scope of the policy 3) outline the roles and responsibilities for granting and denying access 4) provide the framework for the protection of mobile devices against prevailing risks, including users owned devices 5) provide the framework to protect information from unauthorized access and grant access to the appropriate users and mobile devices 6) be documented and communicated to all users 7) be read and acknowledged formally by all users 8) be maintained, reviewed and updated at planned intervals or if significant changes occur		

Implementation Guidance (for information purpose only)

Asset owners should determine appropriate access rules, privileges and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks.

Users and service providers should be given a clear statement of the business requirements to be met by access controls.

The policy should take account of the following:

a. security requirements of individual business applications;
b. policies for information dissemination and authorization, e.g. the need to know principle and security levels and classification of information;
c. consistency between the access rights and information classification policies of different systems and networks;
d. relevant legislation and any contractual obligations regarding protection of access to data or services;
e. management of access rights for users and mobile devices in a distributed and networked environment which recognizes all types of connections available;
f. segregation of access control roles, e.g. access request, access authorization, access administration;
g. requirements for formal authorization of access requests;
h. requirements for periodic review of access controls;
i. removal of access rights related to users and mobile devices;
j. archiving of records of all significant events concerning the use and management of user identities and security credentials;
k. privileged access roles.

When using mobile devices, e.g. notebooks, palmtops, laptops, smart cards, and mobile phones, special care should be taken to ensure that business information is not compromised. The access control policy should take into account the risks of working with mobile computing equipment in unprotected environments.

The mobile related requirements should include physical protection, access controls, cryptographic techniques, backups, and virus protection. This policy should also include rules and advice on connecting mobile devices to networks and guidance on the use of these facilities in public places.

T5.2	User Access Management
Objective	To ensure authorized user access and to prevent unauthorized access to information systems.
Performance Indicator	Number of delayed access change requests, and when they have been actioned.
Automation Guidance	One way of automation is to use identity management systems to manage accounts, their authentication, authorization, roles, and privileges. They are available for entities of all sizes and complexity. Selection of the appropriate identity management system requires an entity to understand its technology landscape, integration requirements, and maturity of its IT staff. Entity should consider which authentication technologies and processes to apply, including smart cards, security tokens, one time passwords, security authentications apps for smartphones, biometric authentication systems, etc.
Relevant Threats and Vulnerabilities	• Use of stolen login credentials • Brute force and dictionary attacks • Authentication bypass

T5.2.1	User Registration	Priority	P1			
		Applicability	Based on risk assessment			
Control	The entity shall implement a formal user registration and de-registration procedure.					
Sub-Control	The entity shall: 1) establish and formalize procedures for the registration and de-registration of users 2) ensure that a separate account is created for each person requiring access, and prohibit sharing of same accounts across multiple users 3) immediately revoke access from users who have changed roles or jobs or left the entity following the established procedure 4) periodically check and revoke access related to temporary and inactive accounts					

Implementation Guidance (for information purpose only)

The access control procedure for user registration and de-registration should include:

a. using unique user IDs to enable users to be linked to and held responsible for their actions; the use of shared IDs should only be permitted where they are necessary for business or operational reasons and should be approved and documented;
b. verifying that the user has authorization from the owner of the information system or service for the use of the information system or service; separate approval for access rights from management may also be appropriate;
c. verifying that the level of access granted is appropriate to the business purpose and is consistent with organizational security policy, e.g. it does not compromise segregation of duties;
d. ensuring service providers do not provide access until authorization procedures have been completed;
e. maintaining a formal record of all persons registered to use systems and service centrally
f. immediately removing or blocking access rights of users who have changed roles or jobs or left the entity;
g. periodically identifying, and removing or blocking, redundant user IDs and redundant and inactive accounts;
h. ensuring that redundant user IDs are not issued to other users.

T5.2.2	Privilege Management	Priority	P1
		Applicability	Based on risk assessment
Control	The entity shall restrict and control the allocation and use of privileges.		
Sub-Control	The entity shall: 1) maintain a record of all allocated privileges 2) never grant users with domain or local administrative privileges 3) ensure that administrator accounts are used only for system administration activities (e.g. no email or web surfing) 4) use two-factor authentication for all administrative access 5) ensure that all administrative access are logged and audited		

Implementation Guidance (for information purpose only)

Multi-user systems that require protection against unauthorized access should have the allocation of privileges controlled through a formal authorization process in accordance with the relevant access control policy. The following steps should be considered:

a. identify privileged access rights associated with each system, e.g. operating system, database and application;
b. privileged access rights should:
- be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy , i.e. the minimum requirement for their functional role only when needed;
- not be granted until the authorization process is complete
- be assigned to a different User ID than the User ID used for day to day work. Regular user activities should not be performed from privileged accounts
c. an authorization process and a record of all privileges allocated should be maintained;
d. requirements for expiry of privileged access rights should be defined;
e. the competences of users with privileged access rights should be reviewed regularly in order to verify if they are in line with their duties;

f. specific procedures should be established and maintained in order to avoid the use of generic administration User IDs, according to systems configuration capabilities;
g. for generic administration User IDs, the confidentiality of security credentials should be maintained when shared (changing them frequently and as soon as possible when a privileged user leaves or changes job, communicating them among privileged users with appropriate mechanisms).

T5.2.3	User Security Credentials Management	Priority	P1
		Applicability	Based on risk assessment
Control	The entity shall control the allocation of user security credentials.		
Sub-Control	The entity shall: 1) establish a user security credential management policy for users and administrators that is appropriate to the purpose of the entity 2) ensure that the policy includes a secure process to provide users with security credentials; policy should also include credential revocation procedure and credential re-allocation. 3) in case of use of security credentials (i.e. passwords) change default security credentials of all systems and applications 4) in case of credentials, always store them in a well-hashed (including "salting") or encrypted format 5) for accessing critical resources/assets, implement credential systems based on multi-factor authentication		
Implementation Guidance (for information purpose only)			

The process should include the following requirements:

a. users should be required to sign a statement to keep personal security credentials confidential and to keep group e.g. security credentials solely within the members of the group; this signed statement could be included in the terms and conditions of employment;
b. when users are required to maintain their own security credentials they should be provided initially with secure temporary security credentials , which they are forced to change immediately;
c. establish procedures to verify the identity of a user prior to providing a new, replacement or temporary security credentials;
d. temporary security credentials should be given to users in a secure manner; the use of external parties or unprotected (clear text) electronic mail messages should be avoided;
e. temporary security credentials should be unique to an individual and should not be guessable;
f. users should acknowledge receipt of security credentials;
g. default vendor security credentials should be altered following installation of systems or software.

T5.2.4	Review of User Access Rights	Priority	P1			
		Applicability	Based on risk assessment			
Control	The entity shall review users' access rights.					
Sub-Control	The entity shall: 1) maintain access right records for all assets, and identify any granted special access 2) establish a access right review procedure to ensure access rights are reviewed periodically or on any changes in users' status 3) periodically check the granted special access to ensure their validity					
Implementation Guidance (for information purpose only)						

The review of access rights should consider the following guidelines:

a. users' access rights should be reviewed at regular intervals and after any changes, such as promotion, demotion or termination of employment;
b. user access rights should be reviewed and re-allocated when moving from one employment to another within the same entity;
c. authorizations for special privileged access rights should be reviewed at more frequent intervals;
d. privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained;
e. changes to privileged accounts should be logged for periodic review.

T5.3	User Responsibilities
Objective	To prevent unauthorized user access, and compromise or theft of information and information systems
Performance Indicator	Percentage of users compliant with the users rules of behavior (such as password policy, clean desk policy)
Automation Guidance	For password management, built-in operating system features for minimum password length can be configured that prevent users from choosing short passwords. To enforce password complexity (requiring passwords to be a string of pseudo-random characters), built-in operating system settings or third-party password complexity enforcement tools can be applied. For critical information and services, two factor authentication systems should be considered.
Relevant Threats and Vulnerabilities	• Intentional leaks and sharing of data by staff • Illegal processing of data • Abuse of system access and/or privileges

T5.3.1	Use of Security Credentials	Priority	P1
		Applicability	Based on risk assessment
Control	The entity shall require users to use security credentials in line with the entity's security practices.		
Sub-Control	The entity shall: 1) develop a good practice for use of security credentials 2) share and educate users on the developed good practices through awareness and training sessions (refer to M3.2.1)		

Implementation Guidance (for information purpose only)

All users should be advised to:

a. keep secret authentication confidential, ensuring that they are not divulged to any other parties, including people of authority;
b. avoid keeping a record (e.g. paper, software file or hand-held device- of security credentials, unless this can be stored securely and the method of storing has been approved (e.g. password vault);
c. change security credentials whenever there is any indication of their possible compromise;
d. when passwords are used as security credentials, select quality passwords with sufficient minimum length which are:
    1- easy to remember;
    2- not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers and dates of birth etc.;
    3- not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);
    4- free of consecutive identical, all-numeric or all-alphabetic characters;
e. change temporary passwords at the first log-on;
f. not share individual user's security credentials;
g. when passwords are used as security credentials in automated logon procedures, these should not be stored without proper protection;
h. not use the same security credentials for business and non-business purposes.

If users need to access multiple services, systems or platforms, and they are required to maintain multiple separate passwords, they should be advised that they may use a single, quality password (see d) for all services where the user is assured that a reasonable level of protection has been established for the storage of the password within each service, system or platform.

T5.4	Network Access Control
Objective	To prevent unauthorized access to networked services
Performance Indicator	Firewall statistics, such as percentage of outbound packets or sessions that are blocked (e.g. attempted access to blacklisted websites; number of potential hacking attacks repelled, categorized into trivial/of some concern/critical)
Automation Guidance	Some entities use commercial tools that evaluate the rule set of network filtering devices to determine whether they are consistent or in conflict, providing an automated sanity check of network filters and search for errors in rule sets or access controls lists (ACLs) that may allow unintended services through the device. Such tools should be run each time significant changes are made to firewall rule sets, router ACLs, or other filtering technologies.
Relevant Threats and Vulnerabilities	• Unauthorized access to network services by internal or external user • KeyLogger / Form-Grabber / Spyware • Tampering in network utilities

T5.4.1	Policy on Use of Network Services	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall provide access to users only to the services that they have been specifically authorized to use.		
Sub-Control	The entity shall: 1) establish a policy for the use of network services that is appropriate to the entity 2) develop the framework for managing the network services and ensure the right level of protection provided against unauthorized access 3) limit user access to the required network services and in line with the developed framework		

Implementation Guidance (for information purpose only)

A policy should be formulated concerning the use of networks and network services. This policy should cover:

a. the networks and network services which are allowed to be accessed;
b. authorization procedures for determining who is allowed to access which networks and networked services;
c. management controls and procedures to protect access to network connections and network services;
d. the means used to access networks and network services (e.g. use of VPN or wireless network);
e. the policy on the use of network services should be consistent with the entities access control policy.

T5.4.2	User Authentication for External Connections	Priority	P1
		Applicability	Based on risk assessment
Control	The entity shall use appropriate authentication methods to control access of remote users.		
Sub-Control	The entity shall: 1) require all remote login (users and administrators) to be done over secure channels 2) ensure appropriate authentication methods to be used to control access by remote users 3) block access to a machine (either remotely or locally) for administrator-level accounts		
Implementation Guidance (for information purpose only)			

Authentication of remote users can be achieved using, for example, a cryptographic based technique, hardware tokens, or a challenge/response protocol. Possible implementations of such techniques can be found in various virtual private networks (VPN solutions). Dedicated private lines can also be used to provide assurance of the source of connections.

Node authentication can serve as an alternative means of authenticating groups of remote users where they are connected to a secure, shared computer facility. Cryptographic techniques, e.g. based on machine certificates, can be used for node authentication. This is part of several VPN based solutions.

T5.4.3	Equipment Identification in Networks	Priority	P1
		Applicability	Based on risk assessment
Control	The entity shall be able to identify equipment connected to its networks.		
Sub-Control	The entity shall: 1) use equipment identification mechanisms to automatically authenticate legitimate connections and detect unauthorized devices connected to the network		
Implementation Guidance (for information purpose only)			

Equipment identification can be used if it is important that the communication can only be initiated from a specific location or equipment. An identifier in or attached to, the equipment can be used to indicate whether this equipment is permitted to connect to the network. These identifiers should clearly indicate to which network the equipment is permitted to connect, if more than one network exists and particularly if these networks are of differing sensitivity. It may be necessary to consider physical protection of the equipment to maintain the security of the equipment identifier.

T5.4.4	Remote Diagnostic and Configuration Protection	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity shall control access for the purpose of diagnostic and configuration.					
Sub-Control	The entity shall: 1) identify all ports and services that are used for diagnostics or configuration 2) disable or uninstall the diagnostic and configuration services that are not required and define a protection mechanism for the ones that are required 3) enable access control mechanisms (including strong authentication) to allow access only to authorized personnel 4) log all remote access activities related to diagnostics and configuration					
Implementation Guidance (for information purpose only)						

Many computer systems, network systems, and communication systems are installed with a remote diagnostic and configuration port or service for use by maintenance engineers. If unprotected, these diagnostic ports provide a means of unauthorized access.

T5.4.5	Network Connection Control	Priority	P1			
		Applicability	Based on risk assessment			
Control	The entity shall restrict user access to shared networks.					
Sub-Control	The entity shall: 1) establish a procedure to provide access to shared networks in line with Access Control Policy and requirements of the business applications (refer to T5.1.1) 2) restrict users access to the network based on predefined tables and rules (e.g. certain time of the day)					
Implementation Guidance (for information purpose only)						

The network access rights of users should be maintained and updated as required by the access control policy. The connection capability of users can be restricted through network gateways that filter traffic by means of pre-defined tables or rules. Examples of applications to which restrictions should be applied are:

a. messaging, e.g. electronic mail;
b. file transfer;
c. interactive access;
d. application access.

Linking network access rights to certain times of day or dates should be considered.

T5.4.6	Network Routing Control	Priority			P3	
		Applicability	Based on risk assessment			
Control	The entity shall implement network routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications.					
Sub-Control	The entity shall: 1) identify all routing equipment (e.g. routers, firewalls, and switches.) (refer to T1.2.1) 2) establish a secure configuration and rules for network routing (refer to T3.2.1) 3) enable source and destination address violation against rules checking on the routing equipment 4) enable routing protection countermeasures to avoid manipulation of routing systems/tables 5) implement sub-networks for publicly accessible systems that are separated from internal organizational networks (refer to T4.5.3) 6) connect to external networks or information systems only through managed interfaces consisting of boundary protection devices (such as firewalls) 7) monitor communications with external systems and with key internal systems for suspicious traffic					

Implementation Guidance (for information purpose only)

Routing controls should be based on positive source and destination address checking mechanisms.

Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected sub-networks). Sub-networks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.

T5.4.7	Wireless Access	Priority		P2		
		Applicability	Based on risk assessment			
Control	The entity shall ensure wireless access is secured.					
Sub-Control	The entity shall: 1) establish usage restrictions, configuration requirements, and implementation guidance for wireless access 2) authorize wireless access to the information system prior to allowing such connections					

Implementation Guidance (for information purpose only)

Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication.

Authentication controls should be implemented to control access to wireless networks. In particular, special care is needed in the selection of controls for wireless networks due to the greater opportunities for undetected interception and insertion of network traffic.

Entities should consider a number of actions to limit unauthorized use of wireless communications outside its boundaries include, for example:

- reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be used by adversaries outside of the physical perimeters of organizations;
- employing measures such as TEMPEST to control wireless emanations; and
- using directional/beam forming antennas that reduce the likelihood that unintended receivers will be able to intercept signals.

Prior to taking such actions, entities can conduct periodic wireless surveys to understand the radio frequency profile of its information systems as well as other systems that may be operating in the area.

T5.5	Operating System Access Control
Objective	To prevent unauthorized access to operating systems
Performance Indicator	Number of blocked attempts at unauthorized access to operating systems
Automation Guidance	Built-in operating system features can extract lists of accounts with super-user privileges, both locally on individual systems and on overall domain controllers. To verify that users with high-privileged accounts do not use such accounts for day-to-day web surfing and e-mail reading, security personnel should periodically gather a list of running processes to determine whether any browsers or e-mail readers are running with high privileges. Such information gathering can be scripted, with short shell scripts searching for a dozen or more different browsers, e-mail readers, and document editing programs running with high privileges on machines. Some legitimate system administration activity may require the execution of such programs over the short term, but long-term or frequent use of such programs with administrative privileges could indicate that an administrator is not adhering to this control. Monitoring tools can provide such information.
Relevant Threats and Vulnerabilities	• Abuse of system access/privileges • Backdoor or Command and Control • Disable or interfere with security controls • Tampering in network utilities

T5.5.1	Secure Log-On Procedures	Priority	P1
		Applicability	Based on risk assessment
Control	The entity shall control access to systems and applications using a secure log-on and log-off procedure.		
Sub-Control	The entity shall: 1) identify the systems, applications and services that require user authentication 2) classify the identified systems, application and services based on the level of protection needed 3) establish the appropriate log-on and log-off procedures to minimize the opportunity for unauthorized access 4) set a maximum session time for logged on users for sensitive systems and applications 5) terminate inactive sessions after a predefined period of inactivity		

Implementation Guidance (for information purpose only)

Even though most applications have secure log-on implemented, a suitable authentication technique should be chosen to substantiate the claimed identity of a user. Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, should be used.

The procedure for logging into a system or application should be designed to minimize the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system or application, in order to avoid providing an unauthorized user with any unnecessary assistance. A good log-on procedure should:

a. not display system or application identifiers until the log-on process has been successfully completed;
b. display a general notice warning that the computer should only be accessed by authorized users;
c. not provide help messages during the log-on procedure that would aid an unauthorized user;
d. validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect;
e. protect against brute force log-on attempts;
f. log unsuccessful and successful attempts;
g. raise a security event if a potential attempted or successful breach of logon controls is detected;
h. display the following information on completion of a successful log-on:
   1- date and time of the previous successful log-on;
   2- details of any unsuccessful log-on attempts since the last successful log-on;
i. not display a password being entered;
j. not transmit passwords in clear text over a network;
k. terminate inactive sessions after a defined period of inactivity, especially in high risk locations such as public or external areas outside the entity's security management or on mobile devices;
l. restrict connection times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.

Connection time controls should be considered for sensitive computer applications, especially from high risk locations, e.g. public or external areas that are outside the entity's security management. Examples of such restrictions include:

a. using predetermined time slots, e.g. for batch file transmissions, or regular interactive sessions of short duration;
b. restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation;
c. considering re-authentication at timed intervals.

A time-out facility should clear the session screen and also, possibly later, close both application and network sessions after a defined period of inactivity. The time-out delay should reflect the security risks of the area, the classification of the information being handled and the applications being used, and the risks related to the users of the equipment.

A limited form of time-out facility can be provided for some systems, which clear the screen and prevents unauthorized access but does not close down the application or network sessions.

T5.5.2	User Identification and Authentication	Priority	P1
		Applicability	Based on risk assessment
Control	The entity shall create a unique identifier (user ID) for each user and implement a suitable authentication technique.		
Sub-Control	The entity shall: 1) provide a unique identifier to each user 2) enable authentication techniques that are suitable to entity 3) ensure all restricted activity are logged with the associated authenticated users		
Implementation Guidance (for information purpose only)			

This control should be applied for all types of users (including technical support personnel, operators, network administrators, system programmers, and database administrators). User IDs should be used to trace activities to the responsible individual. Regular user activities should not be performed from privileged accounts.

In exceptional circumstances, where there is a clear business benefit, the use of a shared user ID for a group of users or a specific job can be used. Approval by management should be documented for such cases. Additional controls may be required to maintain accountability.

Generic IDs for use by an individual should only be allowed either where the functions accessible or actions carried out by the ID do not need to be traced (e.g. read only access), or where there are other controls in place (e.g. password for a generic ID only issued to one staff at a time and logging such instance).

Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, should be used.

T5.5.3	User Credentials Management System	Priority	P1			
		Applicability	Based on risk assessment			
Control	The entity shall implement a system for managing user credentials (i.e. passwords).					
Sub-Control	The user credential management system shall: 1) automate the user credential change procedure ensuring the authenticity of the associate user identity 2) validate that the changed credentials have sufficient strength for their intended use to ensure quality secret authentication 3) set a maximum lifetime and reuse conditions					

Implementation Guidance (for information purpose only)

A management system for user credentials should:

a. enforce the use of individual user IDs and credentials to maintain accountability;
b. allow users to select and change their own credentials and include a confirmation procedure to allow for input errors;
c. enforce a choice of quality credentials;
d. enforce credential changes;
e. force users to change temporary credentials at the first log-on;
f. maintain a record of previous user credentials and prevent re-use;
g. not display credentials on the screen when being entered;
h. store credential files separately from application system data;
i. store and transmit credentials in protected (e.g. encrypted or hashed- form).

T5.5.4	Use of System Utilities	Priority					P4
		Applicability	Based on risk assessment				
Control	The entity shall restrict and control the use of utility programs that might be capable of overriding system and application controls.						
Sub-Control	The entity shall: 1) identify the system utilities and identify the respective appropriate level of protection 2) keep track of the users access rights provided to the system utilities 3) restrict use of utility programs only to authorized personnel 4) monitor the use of utility programs						

Implementation Guidance (for information purpose only)

The following guidelines for the use of system utilities should be considered:

a. use of identification, authentication, and authorization procedures for system utilities;
b. segregation of system utilities from applications software;
c. limitation of the use of system utilities to the minimum practical number of trusted, authorized users;
d. authorization for ad hoc use of systems utilities;
e. limitation of the availability of system utilities, e.g. for the duration of an authorized change;
f. logging of all use of system utilities;
g. defining and documenting of authorization levels for system utilities;
h. removal or disabling of all unnecessary software based utilities and system software;
i. not making system utilities available to users who have access to applications on systems where segregation of duties is required.

T5.6	Application and Information Access Control
Objective	To prevent unauthorized access to information held in application systems
Performance Indicator	Number of blocked attempts at unauthorized access to applications and information
Automation Guidance	Implement an identity management system and integrate it with existing systems where possible to automate the access restrictions based on the entity policies
Relevant Threats and Vulnerabilities	• Unauthorized access by internal or external user • Backdoor or command and control

T5.6.1	Information Access Restriction	Priority	P1			
		Applicability	Based on risk assessment			
Control	The entity shall restrict access to information and application system functions in accordance with the access control policy.					
Sub-Control	The entity shall: 1) ensure access to information and application system functions is restricted 2) ensure access restriction is based on user's roles and responsibilities 3) assign the appropriate level of access rights to information and application functions 4) for each user and support personnel, adjust their access control based on specific business needs					

Implementation Guidance (for information purpose only)

Restrictions to access should be based on individual business application requirements. The access control policy should also be consistent with the organizational access policy.

Applying the following guidelines should be considered in order to support access restriction requirements:

a. providing menus to control access to application system functions;
b. controlling the access rights of users, e.g. read, write, delete, and execute;
c. controlling access rights of other applications;
d. ensuring that outputs from application systems handling sensitive information contain only the information relevant to the use of the output and are sent only to authorized terminals and locations; this should include periodic reviews of such outputs to ensure that redundant information is removed.

T5.6.2	Sensitive System Isolation	Priority		P2		
		Applicability	Based on risk assessment			
Control	The entity shall build a dedicated environment for sensitive systems.					
Sub-Control	The entity shall: 1) identify sensitive applications and allocate the appropriate resources to ensure its security					

Implementation Guidance (for information purpose only)

The following points should be considered for sensitive system isolation:

a. the sensitivity of an application system should be explicitly identified and documented by the application owner;
b. access to sensitive systems in data centers should be restricted by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read or write to such devices
c. when a sensitive application is to run in a shared environment, the application systems with which it will share resources and the corresponding risks should be identified and accepted by the owner of the sensitive application

T5.6.3	Publicly Accessible Content	Priority / Applicability			P3	Based on risk assessment
Control	The entity shall not expose non-public information to the general public.					
Sub-Control	The entity shall: 1) develop and formalize procedures for the publishing of public information to ensure non-public information is not exposed 2) adopt procedures to periodically verify if sensitive information is exposed to the general public					

Implementation Guidance (for information purpose only)

For the publishing of public information, the entity should consider the following:

a. Define publishing procedures with required reviews and approvals for any information to be publicly available
b. Designate individuals authorized to review and post information onto a publicly accessible information system
c. Provide training and awareness sessions for implicated individuals to ensure that publicly accessible information are sanitized from nonpublic information
d. Periodically scan publicly accessible information for non-public information and correct any inconsistency

T5.7	Mobile Devices Access Control
Objective	To ensure information security when using mobile devices
Performance Indicator	Percentage of mobile computing equipment (e.g. smart phones, laptops, tablets) that are fully compliant with the relevant requirements in the access control policy
Automation Guidance	With asset inventory assembled, many entities use tools to pull information from network assets such as switches and routers regarding the machines connected to the network. Using securely authenticated and encrypted network management protocols, tools can retrieve MAC addresses and other information from network devices that can be reconciled with the entity's asset inventory of servers, workstations, laptops, and other devices. Once MAC addresses are confirmed, switches should implement 802.1x and NAC to only allow authorized systems that are properly configured to connect to the network. Going further, effective entities configure free or commercial network scanning tools to perform network sweeps on a regular basis, sending a variety of different packet types to identify devices connected to the network. Before such scanning can take place, entities should verify that they have adequate bandwidth for such periodic scans by consulting load history and capacities for their networks. In conducting inventory scans, scanning tools could send traditional ping packets (ICMP Echo Request) looking for ping responses to identify a system at a given IP address. Because some systems block inbound ping packets, in addition to traditional pings, scanners can also identify devices on the network using transmission control protocol (TCP) synchronize (SYN) or acknowledge (ACK) packets. Once they have identified IP addresses of devices on the network, some scanners provide robust fingerprinting features to determine the operating system type of the discovered machine. In addition to active scanning tools that sweep the network, other asset identification tools passively listen on network interfaces looking for devices to announce their presence by sending traffic. Such passive tools can be connected to switch span ports at critical places in the network to view all data flowing through such switches, maximizing the chance of identifying systems communicating through those switches.
Relevant Threats and Vulnerabilities	• Capture data resident on system • Use of stolen login credentials • Remote spying

T5.7.1	Access Control for Mobile Devices	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity shall adopt the appropriate security measures to protect against the risks of using portable and mobile devices.					
Sub-Control	The entity shall: 1) establish security measures for usage restrictions, configuration/ connection requirements, and implementation guidance for entity-controlled mobile devices in line with the access control policy (See T5.1.1) 2) authorize connection of mobile devices to organizational information systems in accordance with the established security measures					

Implementation Guidance (for information purpose only)

Usage restrictions and implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software- integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Entities are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many relevant safeguards and countermeasures for mobile devices are reflected in the other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process.
The entity should:

1. Prohibit the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official (See T2.2.5); and
2. Enforce the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information:

    1- Connection of unclassified mobile devices to classified information systems is prohibited;
    2- Connection of unclassified mobile devices to unclassified information systems requires approval from the authorizing official;
    3- Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited; and
    4- Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by the assignment security officials, and if classified information is found, the incident handling policy is followed.

Also see T1.2.4 on Acceptable use for BYOD

T5.7.2	Teleworking	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity shall implement security measures to protect information accessed, processed or stored on teleworking sites.					
Sub-Control	The entity shall: 1) establish security measures for using teleworking in line with the access control policy 2) authorize the usage of teleworking in accordance with the established security measures					

Implementation Guidance (for information purpose only)

Entities allowing teleworking activities should establish security measures that define the conditions and restrictions for using teleworking. Where deemed applicable and allowed by law, the following matters should be considered:

a. the existing physical security of the teleworking site, taking into account the physical security of the building and the local environment;
b. the proposed physical teleworking environment;
c. the communications security requirements, taking into account the need for remote access to the entity's internal systems, the sensitivity of the information that will be accessed and pass over the communication link and the sensitivity of the internal system;
d. the provision of virtual desktop access that prevents processing and storage of information on privately owned equipment;
e. the threat of unauthorized access to information or resources from other persons using the accommodation, e.g. family and friends;
f. the use of home networks and requirements or restrictions on the configuration of wireless network services;
g. policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;
h. access to privately owned equipment (to verify the security of the machine or during an investigation), which may be prevented by legislation;
i. software licensing agreements that are such that entities may become liable for licensing for client software on workstations owned privately by employees or external party users;
j. anti-virus protection and firewall requirements.

The guidelines and arrangements to be considered should include:
a. the provision of suitable equipment and storage furniture for the teleworking activities, where the use of privately owned equipment that is not under the control of the entity is not allowed;
b. a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the teleworker is authorized to access;
c. the provision of suitable communication equipment, including methods for securing remote access;
d. physical security;
e. rules and guidance on family and visitor access to equipment and information;
f. the provision of hardware and software support and maintenance;
g. the provision of insurance;
h. the procedures for backup and business continuity;
i. audit and security monitoring;
j. revocation of authority and access rights, and the return of equipment when the teleworking activities are terminated

T6 Third-Party Security

T6	Third Party Security
Objective	To ensure external stakeholders are compliant with an entities security requirements
Performance Indicator	Frequency of information security incidents involving third parties

T6.1	Third Party Security Policy
Objective	To maintain a third party security policy covering the security of acquired services
Performance Indicator	Extent of third party security policy deployment and adoption across the entity
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Unsuitable third party security policy • Unawareness of third party security policy among IT staff

T6.1.1	Third Party Security Policy	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity shall establish a third party security policy to facilitate the implementation of the associated controls.					
Sub-Control	The third party security policy shall: 1) be appropriate to the relationship of the entity and the third party 2) include statement of the management commitment, purpose, objective and scope of the policy 3) outline the roles and responsibilities for managing third parties 4) provide the framework for setting information security objectives and/or include information security objectives to be used when engaging third parties 5) be documented and communicated to the third party 6) be read and acknowledged formally by the third party 7) be maintained, reviewed and updated at planned intervals or if significant changes occur					

Implementation Guidance (for information purpose only)

The third party security policy facilitates the implementation of the associated controls to safeguard the entity's information assets when third parties are involved in their operation. The policy can, for example, contain in addition to the required sub-controls:

a. Third party engagement terms and conditions
b. Information security requirements
c. Audit requirements

The third party security policy can be included as part of the general information security policy, in a single policy document, or can be represented by multiple policies reflecting the complex nature of certain entities.

T6.2	Third Party Service Delivery Management
Objective	To ensure third parties implement and maintain the appropriate level of information security and service delivery
Performance Indicator	Frequency of information security incidents involving third parties
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Abuse of functionality • Data from untrustworthy sources

T6.2.1	Service Delivery	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall monitor third party service delivery.		
Sub-Control	The entity shall: 1) ensure that security requirements for third parties are included in the service delivery agreement for each party 2) ensure these security requirements are measurable 3) require third parties to measure and report to the entity on these service requirements		

Implementation Guidance (for information purpose only)

Service delivery by a third party should include the agreed security arrangements, service definitions, and aspects of service management. In case of outsourcing arrangements, the entity should plan the necessary transitions (of information, information systems, and anything else that needs to be moved), and should ensure that security is maintained throughout the transition period.

The entity should ensure that the third party maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.

T6.2.2	Monitoring and Review of Third Party Services	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall monitor and review the services, reports and records provided by the third party.		
Sub-Control	The entity shall: 1) monitor Use third Party ' services and ensure required delivery reports are received 2) ensure reports received from third parties are reviewed by qualified personnel 3) ensure that information security incidents and problems identified in the reports are managed properly 4) carry out audits for third parties services at a regular basis		

Implementation Guidance (for information purpose only)

Monitoring and review of third party services should involve a service management relationship and process between the entity and the third party to:

a. monitor service performance levels to check adherence to the agreements;
b. review service reports produced by the third party and arrange regular progress meetings as required by the agreements;
c. provide information about information security incidents and review of this information by the third party and the entity as required by the agreements and any supporting guidelines and procedures;
d. review third party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;
e. resolve and manage any identified problems.

The responsibility for managing the relationship with a third party should be assigned to a designated individual or service management team. In addition, the entity should ensure that the third party assigns responsibilities for checking for compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources should be made available to monitor the requirements of the agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed.

The entity should maintain sufficient overall control and visibility into all security aspects for sensitive or critical information or information systems accessed, processed or managed by a third party. The entity should ensure they retain visibility into security activities such as change management, identification of vulnerabilities, and information security incident reporting/response through a clearly defined reporting process, format and structure

T6.2.3	Managing Changes to Third Party Services	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall manage changes to the provision of third party services, including maintaining and improving existing information security policies, procedures and controls.		
Sub-Control	The entity shall: 1) ensure that third party service agreements include a methodology for communicating change management issues between the entity and the third party 2) define the parameters for changes that must be communicated between the entity and the third party 3) assess the changes taking into account the criticality of business systems and processes involved and re-assessment of risks		

Implementation Guidance (for information purpose only)

The process of managing changes to a third party service needs to take account of:

a. changes made by the entity to implement:
   1- enhancements to the current services offered;
   2- development of any new applications and systems;
   3- modifications or updates of the entity's policies and procedures;
   4- new controls to resolve information security incidents and to improve security;

b. changes in third party services to implement:
   1- changes and enhancement to networks;
   2- use of new technologies;
   3- adoption of new products or newer versions/releases;
   4- new development tools and environments;
   5- changes to physical location of service facilities;
   6- change of vendors.

T6.3	Cloud Computing
Objective	To secure information stored, processed, and retrieved through cloud services
Performance Indicator	Percentage of service level agreements capturing all relevant cloud security requirements
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Abuse of functionality • Accidental leaks / sharing of data • Illegal processing of data

T6.3.1	Information Security Requirements for Cloud Environments	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall define information security requirements covering the retention, processing, and storage of data in cloud environments.		
Sub-Control	The entity shall: 1) perform necessary due diligence to determine requirements and restrictions relevant to information processing, storage and retention in the cloud environment 2) include the cloud environment (and, where possible, its components) into the risk assessment process 3) develop and maintain information governance policies and procedures to ensure compliance with identified requirements and risk mitigation strategies 4) ensure information about security incidents that happen at the cloud service provider are communicated 5) where possible, reserve a right to audit the security arrangements in place at cloud service provider		

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard.

A risk-based approach used to establish data security requirements for cloud environments should consider the following:

a. regulatory and other requirements potentially limiting the processing, storage and retention of information in external entities, for example laws or business agreements preventing certain types of information from being stored outside national borders, privacy legislation, and / or regulatory, statutory, contractual, business, and other requirements
b. the complete life cycle of information across entire networks, including both within cloud and non-cloud elements, as well as the interchange of information between these two elements
c. awareness of where sensitive information is stored and transmitted across applications, databases, servers and network infrastructure
d. compliance with defined retention periods and end-of-life disposal requirements

e. information classification and protection from unauthorized use, access, loss, destruction, and falsification
f. balancing the expected benefits of leveraging cloud-based services against the potential risks

T6.3.2	Service Delivery Agreements with Cloud Providers	Priority		P2		
		Applicability	Based on risk assessment			
Control	The entity shall document relevant security requirements in service delivery agreements with cloud service providers.					
Sub-Control	Each service delivery agreement for cloud services shall include provisions for: 1) understanding and maintaining awareness of where information with applicable restrictions will be stored or transmitted in the cloud environment 2) ensuring appropriate information migration plans at the end of the service period 3) ensuring all other cloud security requirements determined relevant by the entity are included in the service delivery agreement					

Implementation Guidance (for information purpose only)

When establishing service delivery agreement for cloud-based services, it is the entity's responsibility to define security requirements for the cloud vendor. This should also take into consideration that the entity may have different levels of ability to negotiate these terms with a vendor based on the type of cloud services being purchased (e.g. private vs. public).

Part of the entity's responsibility includes understanding, where possible, where information will be stored, processed, or transmitted to ensure that often sensitive information privacy laws and other legal restrictions (e.g. prohibiting transmission of certain types of information outside national borders) are respected.

In addition, the entity should ensure that the terms and conditions of service delivery agreements provide ample clarification on how information will be migrated from the selected cloud service provider to another provider (or back to the entity) at the termination of the service delivery agreement. This is critical to ensuring that the entity is not "held hostage" by the service provider.

T7 Information Systems Acquisition, Development and Maintenance

T7	Information Systems Acquisition, Development and Maintenance
Objective	To prevent information misuse or unauthorized modification and to elevate security levels in applications, during development as well as to manage technical vulnerabilities
Performance Indicator	Percentage of information systems compliant to information systems acquisition, development and maintenance policy

T7.1	Information Systems Acquisition, Development and Maintenance Policy
Objective	To maintain an information systems acquisition, development and maintenance policy covering the security of information systems throughout its lifecycle
Performance Indicator	Extent of information systems acquisition, development and maintenance policy deployment and adoption across the entity
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Unsuitable information systems acquisition, development and maintenance policy • Partial information systems acquisition, development and maintenance policy not covering the entire asset lifecycle

T7.1.1	Information Systems Acquisition, Development and Maintenance Policy	Priority					P4
		Applicability	Based on risk assessment				
Control	The entity shall establish an information systems acquisition, development, and maintenance policy.						
Sub-Control	The information systems acquisition, development, and maintenance policy shall: 1) be appropriate to the relationship of the entity and all internal and external parties involved in the process 2) include statement of the management commitment, purpose, objective and scope of the policy 3) outline the roles and responsibilities 4) provide the framework for setting information security objectives and/or include information security objectives to be used when engaging in the process 5) be documented and communicated to all users 6) be read and acknowledged formally by all users 7) be maintained, reviewed and updated at planned intervals or if significant changes occur						

Implementation Guidance (for information purpose only)

The information systems acquisition, development and maintenance policy facilitates the implementation of the associated controls to integrate information security requirements into the software life cycle of information systems that contain protected data. The policy can, for example, contain in addition to the required sub-controls:

a. Information security requirements around systems specification, correct processing, cryptography, system files, etc.
b. Audit requirements

The information systems acquisition, development and maintenance policy can be included as part of the general information security policy, in a single policy document, or can be represented by multiple policies reflecting the complex nature of certain entities.

T7.2	Security Requirements of Information Systems
Objective	To ensure that security requirements are established and functionally integrated into information systems
Performance Indicator	Percentage of systems implementations accepted into service with all security requirements implemented
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Equipment malfunction • Abuse of functionality

T7.2.1	Security Requirements Analysis and Specification	Priority			P3	
		Applicability	Based on risk assessment			
Control	The entity shall develop information security requirements for new information systems or enhancements to existing information systems.					
Sub-Control	The security requirements shall: 1) be used for new information systems or enhancements to existing information systems 2) be approved by the appropriate business manager or equivalent 3) address all requirements for security controls identified during the risk assessment 4) outline how to verify that the requirements for security controls have been met 5) be included in the statement of business and technical requirements					

Implementation Guidance (for information purpose only)

Information security requirements should be identified using various methods such as and policies, reviews threat modeling and vulnerability thresholds/vulnerably remediation. Results from the identification should be documented merging views of all stakeholders.

Security requirements and controls should reflect the business value of the information involved and the potential negative business impact which might result from lack of adequate security.
System requirements for information security and processes for implementing security should be integrated in the early stages of information system projects. Controls introduced at the design stage are significantly cheaper to implement and maintain than those included during or after implementation. The sizing of information systems should take into account enabling all security features in that system; i.e. higher specifications model of Security-Systems so that when security features are enabled they do not cause slow-down and degradation in the information systems performance.

For applications systems providing services or transferring information over public networks, the system requirements should also consider the following:

a. the level of confidence each party requires in each other's claimed identity, e.g. through authentication;
b. authorization processes associated with who may approve contents of, issuing or signing key transactional documents;
c. ensuring that communicating partners are fully informed of their authorizations for provision or use of the service;
d. determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents and the non-repudiation of contracts, e.g. associated with tendering and contract processes;
e. the level of trust required in the integrity of key documents;
f. the confidentiality of any confidential information;
g. the confidentiality and integrity of any order transactions, payment information, delivery address details and confirmation of receipts;
h. the degree of verification appropriate to verify payment information supplied by a customer;
i. selecting the most appropriate settlement form of payment to guard against fraud;
j. the level of protection required to maintain the confidentiality and integrity of order information;
k. avoidance of loss or duplication of transaction information;
l. liability associated with any fraudulent transactions;
m. insurance requirements;
n. transaction related requirements such as authenticity, confidentiality and integrity of transaction related data, non-repudiation and protection of any transaction related data.

If products are acquired, a formal testing and acquisition process should be followed. Contracts with the supplier should address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement then the risk introduced and associated controls should be reconsidered prior to purchasing the product.
Available guidance for security configuration of the product aligned with the final software / service stack of that system should be evaluated and implemented.

Criteria for accepting products should be defined e.g., in terms of their functionality, which give assurance that the identified security requirements are met. Products should be evaluated against these criteria before acquisition. Where additional functionality is supplied and causes a security risk, this should be disabled or the proposed control structure should be reviewed to determine if advantage can be taken of the enhanced functionality available.

T7.2.2	Developer-Provided Training	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity shall require the developer of the information system, system component, or information system service to provide the trainings needed.					
Sub-Control	The entity shall require the developer to: 1) identify training requirements based on implemented security functions and in line with the Awareness and Training Policy (refer to M3.1.1) for the correct use and operation of the functions 2) design and execute appropriate training programs to meet these requirements 3) include training provisions in the relevant service delivery agreement					

Implementation Guidance (for information purpose only)

This control applies to external and internal (in-house- developers). Training of personnel is an essential element to ensure the effectiveness of security controls implemented within organizational information systems. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training. Entities can also request sufficient training materials from developers to conduct in-house training or offer self-training to organizational personnel. Entities determine the type of training necessary and may require different types of training for different security functions, controls, or mechanisms.

T7.3	Correct Processing in Applications
Objective	To prevent errors, loss, unauthorized modification or misuse of information in applications
Performance Indicator	Percentage of systems for which data validation controls have been adequately defined, implemented, and proven effective by thorough testing
Automation Guidance	Source code testing tools, web application security scanning tools, and object code testing tools have proven useful in securing application software, along with manual application security penetration testing by testers who have extensive programming knowledge and application penetration testing expertise. The Common Weakness Enumeration (CWE) initiative is used by many such tools to identify the weaknesses that they find. Entities can also use CWE to determine which types of weaknesses they are most interested in addressing and removing. When evaluating the effectiveness of testing for these weaknesses, MITRE's Common Attack Pattern Enumeration and Classification can be used to organize and record the breadth of the testing for the CWEs and to enable testers to think like attackers in their development of test cases.
Relevant Threats and Vulnerabilities	• Software malfunction • Illegal processing of data • Injection flaws, such as SQL, OS, and LDAP • Broken Authentication and Session Management • Cross-Site Scripting (XSS)

T7.3.1	Input Data Validation	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall validate data input to applications to ensure that this data is correct and appropriate.		
Sub-Control	The entity shall: 1) define a set of guidelines or parameters to be used to validate data input into applications 2) define a set of values for each guideline or parameter to identify acceptable and unacceptable values 3) provide guidance on how to validate each guideline or parameter		

Implementation Guidance (for information purpose only)

Checks should be applied to the input of business transactions, standing data (e.g. names and addresses, credit limits, customer reference numbers), and parameter tables (e.g. sales prices, currency conversion rates, tax rates). The following guidelines should be considered:

a. dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data, to detect the following errors:
   1- out-of-range values;
   2- invalid characters in data fields;
   3- missing or incomplete data;
   4- exceeding upper and lower data volume limits;
   5- unauthorized or inconsistent control data;

b. periodic review of the content of key fields or data files to confirm their validity and integrity;
c. inspecting hard-copy input documents for any unauthorized changes (all changes to input documents should be authorized);
d. procedures for responding to validation errors;
e. procedures for testing the plausibility of the input data;
f. defining the responsibilities of all personnel involved in the data input process;
g. creating a log of the activities involved in the data input process

T7.3.2	Control of Internal Processing	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall incorporate validation checks into applications to detect any corruption of information through processing errors or deliberate acts.		
Sub-Control	The entity shall: 1) provide guidelines to application developers on minimum requirements for validation checks for applications under development 2) require application developers to provide evidence of compliance with minimum requirements 3) periodically review existing applications to ensure validation checks included during their development still met minimum requirements		

Implementation Guidance (for information purpose only)

The design and implementation of applications should ensure that the risks of processing failures leading to a loss of integrity are minimized. Specific areas to consider include:

a. the use of add, modify, and delete functions to implement changes to data;
b. the procedures to prevent programs running in the wrong order or running after failure of prior processing;
c. the use of appropriate programs to recover from failures to ensure the correct processing of data;
d. protection against attacks using buffer overruns/overflows.

An appropriate checklist should be prepared, activities documented, and the results should be kept secure. Examples of checks that can be incorporated include the following:

a. session or batch controls, to reconcile data file balances after transaction updates;
b. balancing controls, to check opening balances against previous closing balances, namely:
   1- run-to-run controls;
   2- file update totals;
   3- program-to-program controls;

c. validation of system-generated input data;
d. checks on the integrity, authenticity or any other security feature of data or software downloaded, or uploaded, between central and remote computers;
e. hash totals of records and files;
f. checks to ensure that application programs are run at the correct time;
g. checks to ensure that programs are run in the correct order and terminate in case of a failure, and that further processing is halted until the problem is resolved;
h. creating a log of the activities involved in the processing.

T7.3.3	Message Integrity	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall ensure authenticity and integrity of messages in applications.		
Sub-Control	The entity shall: 1) identify requirements to ensure authenticity and integrity of messages transmitted between systems and applications 2) adopt proper controls to address the identified requirements		

Implementation Guidance (for information purpose only)

An assessment of security risks should be carried out to determine if message integrity is required and to identify the most appropriate method of implementation. Proper technical countermeasures (as hashing/ digital signature)should be adopted to ensure integrity of messages during their transmission.

T7.3.4	Output Data Validation	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall validate data output from an application		
Sub-Control	The entity shall: 1) define output validation procedures to ensure that the processing of stored information is correct and appropriate to the circumstances		

Implementation Guidance (for information purpose only)

Output validation may include:

a. plausibility checks to test whether the output data is reasonable;
b. reconciliation control counts to ensure processing of all data;
c. providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information;
d. procedures for responding to output validation tests;
e. defining the responsibilities of all personnel involved in the data output process;
f. creating a log of activities in the data output validation process.

T7.4	Cryptographic controls
Objective	To protect the confidentiality, authenticity or integrity of information by cryptographic means.
Performance Indicator	Percentage of systems containing valuable/sensitive data for which suitable cryptographic controls have been fully implemented
Automation Guidance	Cryptography can only be performed through the use of automated cryptographic systems. These systems should automate all processes, including key generation, distribution, revocation, restoration, etc.
Relevant Threats and Vulnerabilities	• Weak cryptography used for sensitive data • Eavesdropping / Packet sniffing Sensitive Data Exposure

T7.4.1	Policy on the Use of Cryptographic Controls	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall establish a policy on the use of cryptographic controls		
Sub-Control	The entity shall: 1) develop and document a policy for the use of cryptographic controls in line with the criticality of the information to be protected 2) ensure the policy takes into account the sector or national level restrictions including TRA's relevant issuances and guidance in this regard 3) share the policy with relevant users 4) review and update the policy at planned intervals or if significant changes occur		

Implementation Guidance (for information purpose only)

When developing a cryptographic policy the following should be considered:

a. the management approach towards the use of cryptographic controls across the entity, including the general principles under which business information should be protected;
b. based on a risk assessment, the required level of protection should be identified taking into account the type, strength, and quality of the encryption algorithm required;
c. the use of encryption for protection of sensitive information transported by mobile or removable media, devices or across communication lines;
d. the approach to key management, including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys;
e. roles and responsibilities, e.g. who is responsible for:
1- the implementation of the policy;
2- the key management, including key generation;
f. these to be adopted for the effective implementation throughout the entity (which solution is used for which business processes);
g. the impact of using encrypted information on controls that rely upon content inspection (e.g. virus detection);
h. any other TRA's relevant issuances, guidance, and activities in this regard

When implementing the entity's cryptographic policy, consideration should be given to the and national restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information.

Cryptographic controls can be used to achieve different security objectives, e.g.:

- confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;
- integrity/authenticity: using digital signatures or message authentication codes to protect the authenticity and integrity of stored or transmitted sensitive or critical information;
- non-repudiation: using cryptographic techniques to obtain proof of the occurrence or non-occurrence of an event or action.

Cryptographic techniques can also be used to implement the dissemination rules of information sharing, e.g. through information rights management.

T7.4.2	Key Management	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall establish key management to support the entity's use of cryptographic techniques.		
Sub-Control	The entity shall: 1) develop a key management policy and process to control the generation of keys taking into account TRA's issuances with regard to key management 2) define key storing standards 3) define procedures to revoke/block keys and to repair damage or corrupted keys 4) protect all cryptographic keys against modification and loss 5) protect secret and private keys against unauthorized use and disclosure		

Implementation Guidance (for information purpose only)

All cryptographic keys should be protected against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorized disclosure. Equipment used to generate, store and archive keys should be physically protected.

A key management system should be based on an agreed set of standards, procedures, and secure methods for:

a. generating keys for different cryptographic systems and different applications;
b. generating and obtaining public key certificates;
c. distributing keys to intended users, including how keys should be activated when received;
d. storing keys, including how authorized users obtain access to keys;
e. changing or updating keys including rules on when keys should be changed and how this will be done;
f. dealing with compromised keys;
g. revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an entity (in which case keys should also be archived);
h. recovering keys that are lost or corrupted as part of business continuity management, e.g. for recovery of encrypted information;
i. archiving keys, e.g. for information archived or backed up;
j. destroying keys;
k. logging and auditing of key management related activities.

In order to reduce the likelihood of compromise, activation, and deactivation dates for keys should be defined so that the keys can only be used for a limited period of time. This period of time should be dependent on the circumstances under which the cryptographic control is being used, and the perceived risk.

In addition to securely managing secret and private keys, the authenticity of public keys should also be considered. This authentication process can be done using public key certificates which are normally issued by a certification authority, which should be a recognized entity with suitable controls and procedures in place to provide the required degree of trust.
The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services.

T7.5	Security of System Files
Objective	To ensure the security of system files
Performance Indicator	Percentage of systems assessed as fully compliant with the information systems acquisition, development and maintenance policy
Automation Guidance	Security of system files can only be achieved through the use of automated controls, including but not limited to file permission restrictions, file access log, and file hashing for integrity check.
Relevant Threats and Vulnerabilities	• Unauthorized access to system files • Corruption of data

T7.5.1	Control of Operational Software	Priority					P4
		Applicability	Based on risk assessment				
Control	The entity shall control the installation of software on operational systems.						
Sub-Control	The entity shall: 1) allow the installation of software only by authorized administrators 2) inhibit installation of software by users, unless justified by their role/ business need 3) keep an original copy of every installed software, including previous versions 4) have a rollback strategy 5) have an audit log of all software installations						

Implementation Guidance (for information purpose only)

To minimize the risk of corruption to operational systems, the following guidelines should be considered to control changes:

a. the updating of the operational software, applications, and program libraries should only be performed by trained administrators upon appropriate management authorization;
b. operational systems should only hold approved executable code, and not development code or compilers;
c. applications and operating system software should only be implemented after extensive and successful testing; the tests should include tests on usability, security, effects on other systems and user-friendliness, and should be carried out on separate systems; it should be ensured that all corresponding program source libraries have been updated;
d. a configuration control system should be used to keep control of all implemented software as well as the system documentation;
e. a rollback strategy should be in place before changes are implemented;
f. an audit log should be maintained of all updates to operational program libraries;
g. previous versions of application software should be retained as a contingency measure;
h. old versions of software should be archived, together with all required information and parameters, procedures, configuration details, and supporting software for as long as the data is retained in archive.

Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The entity should consider the risks of relying on unsupported software.

Any decision to upgrade to a new release should take into account the business requirements for the change, and the security of the release, i.e. the introduction of new security functionality or the number and severity of security problems affecting this version. Software patches should be applied when they can help to remove or reduce security weaknesses.

Physical or logical access should only be given to suppliers for support purposes when necessary, and with management approval. The supplier's activities should be monitored. Computer software may rely on externally supplied software and modules, which should be monitored and controlled to avoid unauthorized changes, which could introduce security weaknesses.

T7.5.2	Protection of System Test Data	Priority			P3	
		Applicability	Based on risk assessment			
Control	The entity shall ensure the protection of system test data.					
Sub-Control	The entity shall: 1) use sample data sets to test data applications 2) limit the transfer of real data from production environment to the test environment, and to be done only after the appropriate authorization 3) erase any data from test applications immediately after testing is completed 4) keep track of any copy/erase of data between production and testing environment					

Implementation Guidance (for information purpose only)

The use of operational databases containing personal information or any other sensitive information for testing purposes should be avoided. If personal or otherwise sensitive information is used for testing purposes, all sensitive details and content should be removed or modified beyond recognition before use. The following guidelines should be applied to protect operational data, when used for testing purposes:

a. the access control procedures, which apply to operational application systems, should also apply to test application systems;
b. there should be separate authorization each time operational information is copied to a test application system;
c. operational information should be erased from a test application system immediately after the testing is complete;
d. the copying and use of operational information should be logged to provide an audit trail.

T7.5.3	Access Control to Program Source Code	Priority				P3	
		Applicability	Based on risk assessment				
Control	The entity shall restrict the access to program source code.						
Sub-Control	The entity shall: 1) define an access control policy to source code 2) define and periodically review permissions 3) keep an audit log of all accesses						

Implementation Guidance (for information purpose only)

Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) should be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes. For program source code, this can be achieved by controlled central storage of such code, preferably in program source libraries. The following guidelines should then be considered to control access to such program source libraries in order to reduce the potential for corruption of computer programs:

a. where possible, program source libraries should not be held in operational systems;
b. the program source code and the program source libraries should be managed according to established procedures;
c. support personnel should not have unrestricted access to program source libraries;
d. the updating of program source libraries and associated items, and the issuing of program sources to programmers should only be performed after appropriate authorization has been received;
e. program listings should be held in a secure environment;
f. an audit log should be maintained of all accesses to program source libraries;
g. maintenance and copying of program source libraries should be subject to strict change control procedures.

T7.6	Security in Development and Support Processes
Objective	To maintain the security of application system software and information
Performance Indicator	Number of cases where the change management processes have not been executed correctly
Automation Guidance	Entity should adopt technical solutions to monitor application and program changes/updates
Relevant Threats and Vulnerabilities	• Unsuitable security for development and support processes • Lack of proper technical review of applications after operating system changes • Leakage of information

T7.6.1	Change Control Procedures	Priority			P3	
		Applicability	Based on risk assessment			
Control	The entity shall control the implementation of changes by the use of formal change control procedures.					
Sub-Control	The entity shall: 1) develop a change control procedure 2) keep track record of all changes 3) keep a copy of every version of the software, adopting appropriate integrity verification procedures 4) ensure all relevant documentations are up-to-date 5) ensure proper planning to perform changes implementation at the right time					

Implementation Guidance (for information purpose only)

Formal change control procedures should be documented and enforced in order to minimize the corruption of information systems. Introduction of new systems and major changes to existing systems should follow a formal process of documentation, specification, testing, quality control, and managed implementation.

This process should include a risk assessment, analysis of the impacts of changes, and specification of security controls needed. This process should also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained.

Wherever practicable, application and operational change control procedures should be integrated. The change procedures should include:

a. maintaining a record of agreed authorization levels;
b. ensuring changes are submitted by authorized users;
c. reviewing controls and integrity procedures to ensure that they will not be compromised by the changes;
d. identifying all software, information, database entities, and hardware that require amendment;
e. obtaining formal approval for detailed proposals before work commences;
f. ensuring authorized users accept changes prior to implementation;
g. ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of;
h. maintaining a version control for all software updates;
i. maintaining an audit trail of all change requests;
j. ensuring that operating documentation and user procedures are changed as necessary to remain appropriate;
k. ensuring that the implementation of changes takes place at the right time and does not disturb the business processes involved.

T7.6.2	Technical Review of Applications After Operating System Changes	Priority			P3	
		Applicability	Based on risk assessment			
Control	The entity shall review and test business critical applications after changes in the operating systems.					
Sub-Control	The entity shall: 1) test any application in a testing environment when operating systems are changed (including patches and configurations) 2) monitor operating system and application logs for any anomaly 3) always define a rollback procedure 4) ensure that changes are reflected in any asset database and in any technical contingency plan					

Implementation Guidance (for information purpose only)

This process should cover:

a. review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes;
b. ensuring that the annual support plan and budget will cover reviews and system testing resulting from operating system changes;
c. ensuring that notification of operating system changes is provided in time to allow appropriate tests and reviews to take place before implementation;
d. ensuring that appropriate changes are made to the business continuity plans.

A specific group or individual should be given responsibility for monitoring vulnerabilities and vendors' releases of patches and fixes.

T7.6.3	Restrictions on Changes to Software Packages	Priority		P2		
		Applicability	Based on risk assessment			
Control	The entity shall restrict the changes to software packages.					
Sub-Control	The entity shall: 1) define who is entitled to approve changes to software/applications 2) test any change in a testing environment before moving it to production environment 3) in case of major changes in critical software and applications, perform a Secure Code Review					

Implementation Guidance (for information purpose only)

As far as possible, and practicable, vendor-supplied software packages should be used without modification.

Where a software package needs to be modified the following points should be considered:

a. the risk of built-in controls and integrity processes being compromised;
b. whether the consent of the vendor should be obtained;
c. the possibility of obtaining the required changes from the vendor as standard program updates;
d. the impact if the entity becomes responsible for the future maintenance of the software as a result of changes.

If changes are necessary the original software should be retained and the changes applied to a clearly identified copy. A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software. All changes should be fully tested and documented, so that they can be reapplied if necessary to future software upgrades. If required, the modifications should be tested and validated by an independent evaluation body.

T7.6.4	Information Leakage	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall prevent opportunities for information leakage.		
Sub-Control	The entity shall: 1) adopt Data Leak Prevention (DLP) measures 2) adopt identity and access management solutions to limit access to critical data only to authorized personnel 3) define and enforce a data/information classification policy		

Implementation Guidance (for information purpose only)

The following should be considered to limit the risk of information leakage, e.g. through the use and exploitation of covert channels:

a- scanning of outbound media and communications for hidden information;
b- masking and modulating system and communications behavior to reduce the likelihood of a third party being able to deduce information from such behavior;
c- making use of systems and software that are considered to be of high integrity, e.g. using evaluated products;
d- regular monitoring of personnel and system activities, where permitted under existing legislations or Regulations;
e- monitoring resource usage in computer systems.

T7.6.5	Outsourced Software Development	Priority			P3	
		Applicability	Based on risk assessment			
Control	The entity shall supervise outsourced software development.					
Sub-Control	The entity shall: 1) define a secure coding policy 2) define a Quality Assurance (QA) process 3) include in the software acquisition contract a clause to oblige third part to be compliant to Entity secure coding policy, to align to Entity QA process; contract shall also include the possibility to conduct audit on the third party 4) specify in the software development contract any requirement and information security functionality 5) conduct a source code review to identify potential vulnerabilities and/or malicious code or code that does not conform to the functionalities required					

Implementation Guidance (for information purpose only)

Where software development is outsourced, the following points should be considered:

a. licensing arrangements, code ownership, and intellectual property rights;
b. certification of the quality and accuracy of the work carried out;
c. escrow arrangements in the event of failure of the third party;
d. rights of access for audit of the quality and accuracy of work done;
e. contractual requirements for quality and security functionality of code;
f. testing before installation to detect malicious and Trojan code.

T7.7	Technical Vulnerability Management
Objective	To reduce risks resulting from exploitation of published or identified technical vulnerabilities
Performance Indicator	Percentage of identified vulnerabilities mitigated within the acceptable time periods as defined in security requirements
Automation Guidance	A large number of vulnerability scanning tools are available to evaluate the security configuration of systems. Some entities have also found commercial services using remotely managed scanning appliances to be effective. To help standardize the definitions of discovered vulnerabilities in multiple departments of an entity or even across entities it is preferable to use vulnerability scanning tools that measure security flaws and map them to vulnerabilities and issues categorized using one or more of the following industry-recognized vulnerability, configuration, and platform classification schemes and languages: CVE, CCE, OVAL, CPE, CVSS, and/or XCCDF. Advanced vulnerability scanning tools can be configured with user credentials to log in to scanned systems and perform more comprehensive

	scans than can be achieved without login credentials. The frequency of scanning activities, however, should increase as the diversity of an entity's systems increases to account for the varying patch cycles of each vendor. In addition to the scanning tools that check for vulnerabilities and misconfigurations across the network, various free and commercial tools can evaluate security settings and configurations of local machines on which they are installed. Such tools can provide fine-grained insight into unauthorized changes in configuration or the inadvertent introduction of security weaknesses by administrators. Effective entities link their vulnerability scanners with problem-ticketing systems that automatically monitor and report progress on fixing problems, and that make unmitigated critical vulnerabilities visible to higher levels of management to ensure the problems are solved. The most effective vulnerability scanning tools compare the results of the current scan with previous scans to determine how the vulnerabilities in the environment have changed over time. Security personnel use these features to conduct vulnerability trending from month to month. As vulnerabilities related to unpatched systems are discovered by scanning tools, security personnel should determine and document the amount of time that elapses between the public release of a patch for the system and the occurrence of the vulnerability scan. If this time window exceeds the entity's benchmarks for deployment of the given patch's criticality level, security personnel should note the delay and determine if a deviation was formally documented for the system and its patch. If not, the security team should work with management to improve the patching process. Additionally, some automated patching tools may not detect or install certain patches due to error by the vendor or administrator. Because of this, all patch checks should reconcile system patches with a list of patches each vendor has announced on its website.
Relevant Threats and Vulnerabilities	• Exploitation of known system vulnerabilities • Undetected system vulnerabilities • Unpatched applications

T7.7.1	Control of Technical Vulnerabilities	Priority	P1
		Applicability	Based on risk assessment
Control	The entity shall obtain and act upon information about technical vulnerabilities of information systems being used		
Sub-Control	The entity shall: 1) identify vulnerabilities in new systems and applications and define a remediation plan before placing them in a production environment 2) test, review, check, and verify the presence of vulnerabilities in production systems throughout the development life-cycle, preferably by the use of automated testing tools 3) perform a Cost-Benefit-Analysis (CBA) for vulnerabilities to determine the proper remediation plan, where appropriate		

Implementation Guidance (for information purpose only)

As a prerequisite, a current and complete inventory of assets is needed (including software vendor, version numbers, current state of deployment, and the person(s) within the entity responsible for the software).

The following guidance should be followed to establish an effective management process for technical vulnerabilities:

a. the entity should define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment (see M2.2), patching, asset tracking, and any coordination responsibilities required;
b. the entity should identify information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them should be identified for software and other technology (based on the asset inventory list); these information resources should be updated based on changes in the inventory, or when other new or useful resources are found;
c. the entity should define a timeline to react to notifications of potentially relevant technical vulnerabilities;
d. the entity should identify the risks associated to potential technical vulnerability and the actions to be taken; such action could involve patching of vulnerable systems and/or applying other controls;
e. depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the controls related to change management or by following information security incident response procedures;
f. if a patch is available, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch);
g. patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered, such as:
    1- turning off services or capabilities related to the vulnerability;
    2- adapting or adding access controls, e.g. firewalls, at network borders;
    3- increased monitoring to detect or prevent actual attacks;
    4- raising awareness of the vulnerability;

h. an audit log should be kept for all procedures undertaken;
i. the technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency;
j. systems at high risk should be addressed first.

T7.8	Supply Chain Management
Objective	To protect against supply chain threats and secure the supply of information systems
Performance Indicator	Percentage of information systems received within the acceptable time frame and validated as genuine Number of vendors/third parties compliant with the policy for acquisition of products and services
Automation Guidance	An automated support system should be used to support tracking of products and services received and verification of compliance to entity policies
Relevant Threats and Vulnerabilities	• Unsuitable supply chain strategy • Use of counterfeit or copied software

T7.8.1	Supply Chain Protection Strategy	Priority					P4
		Applicability	Based on risk assessment				
Control	The entity shall develop a comprehensive information security strategy against supply chain threats to the information assets.						
Sub-Control	The entity shall: 1) define a policy to regulate the acquisition of products and services. Such a policy shall include not to disclose to the supplier any unnecessary details about the entity's configurations and architectures 2) check for every product/service delivered its compliance to security requirements defined by the policy 3) define in the contract with the supplier that compliance with the entity security policy is required 4) incentivize transparency into the security practices of the supplier 5) include the possibility to audit the supplier's security practices 6) ensure all sector and national level requirements for supply chain security are met						

Implementation Guidance (for information purpose only)

The use of acquisition and procurement processes by entities early in the system development life cycle provides an important vehicle to protect the supply chain. Entities use available all-source intelligence analysis to inform the tailoring of acquisition strategies, tools, and methods. There are a number of different tools and techniques available (e.g., obscuring the end use of an information system or system component, using blind or filtered buys). Entities also consider creating incentives for suppliers who:

a. implement required security controls;
b. promote transparency into their organizational processes and security practices;
c. provide additional vetting of the processes and security practices of subordinate suppliers, critical information system components, and services;
d. restrict purchases from specific suppliers or countries; and
e. provide contract language regarding the prohibition of tainted or counterfeit components.

In addition, entities consider minimizing the time between purchase decisions and required delivery to limit opportunities for adversaries to corrupt information system components or products. Finally, entities can use trusted/controlled distribution, delivery, and warehousing options to reduce supply chain risk (e.g., requiring tamper-evident packaging of information system components during shipping and warehousing).

T7.8.2	Supplier Reviews	Priority / Applicability	P4 — Based on risk assessment
Control	The entity shall conduct a supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service.		
Sub-Control	The entity shall: 1) define an evaluation process for suppliers of information systems, system components and services 2) periodically review supplier evaluations 3) ensure the supplier review process includes checks with appropriate sector and national level requirements		

Implementation Guidance (for information purpose only)

Supplier reviews include, for example:

a. analysis of supplier processes used to design, develop, test, implement, verify, deliver, and support information systems, system components, and information system services; and
b. assessment of supplier training and experience in developing systems, components, or services with the required security capability.

These reviews provide entities with increased levels of visibility into supplier activities during the system development life cycle to promote more effective supply chain risk management. Supplier reviews can also help to determine whether primary suppliers have security controls in place and a practice for vetting subordinate suppliers, for example, second- and third-tier suppliers, and any subcontractors.

T7.8.3	Limitation of Harm	Priority / Applicability	P4 — Based on risk assessment
Control	The entity shall limit harm from potential adversaries targeting the organizational supply chain.		
Sub-Control	The entity shall: 1) limit information shared with suppliers 2) employ a diverse set of suppliers for any critical information system product and service area		

Implementation Guidance (for information purpose only)

Supply chain risk is part of the advanced persistent threat. Security controls to reduce the probability of adversaries successfully identifying and targeting the supply chain include, for example:

a. avoiding the purchase of custom configurations to reduce the risk of acquiring information systems, components, or products that have been corrupted via supply chain actions targeted at specific entities;
b. employing a diverse set of suppliers to limit the potential harm from any given supplier in the supply chain; and
c. using procurement carve outs.

T7.8.4	Supply Chain Operations Security	Priority / Applicability	P4 / Based on risk assessment
Control	The entity shall employ security controls to protect supply chain operations.		
Sub-Control	The entity shall: 1) evaluate risks to its own information systems/services operations considering also threats/vulnerabilities relate to suppliers 2) work with suppliers to align controls and have them reported in the service contract 3) define how controls implemented by suppliers will be monitored by the entity		

Implementation Guidance (for information purpose only)

Supply chain information includes, for example: user identities; uses for information systems, information system components, and information system services; supplier identities; supplier processes; security requirements; design specifications; testing and evaluation results; and system/component configurations. This control enhancement expands the scope of operations security (OPSEC) to include suppliers and potential suppliers. OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to operations and other activities to:

a. identify those actions that can be observed by potential adversaries;
b. determine indicators that adversaries might obtain that could be interpreted or pieced together to derive critical information in sufficient time to cause harm to entities;
c. implement controls or countermeasures to eliminate or reduce to an acceptable level, exploitable vulnerabilities; and
d. consider how aggregated information may compromise the confidentiality of users or uses of the supply chain.

OPSEC may require entities to withhold critical mission/business information from suppliers and may include the use of intermediaries to hide the end use, or users, of information systems, system components, or information system services.

T7.8.5	Reliable Delivery	Priority					P4
		Applicability	Based on risk assessment				
Control	The entity shall ensure a reliable delivery of information systems or system components.						
Sub-Control	The entity shall: 1) ensure information systems and components received are genuine 2) verify software delivered has not being altered						

Implementation Guidance (for information purpose only)

For some information system components, especially hardware, there are technical means to help determine if the components are genuine or have been altered. Security controls used to validate the authenticity of information systems and information system components include, for example, optical/ nanotechnology tagging and side-channel analysis, hashes comparison mechanisms also can be used to verify if vender or third party software has been altered or not. For hardware, detailed bill of material information can highlight the elements with embedded logic complete with component and production location.

T7.8.6	Processes to Address Weaknesses or Deficiencies	Priority					P3
		Applicability	Based on risk assessment				
Control	The entity shall establish a process to address weaknesses or deficiencies in supply chain elements.						
Sub-Control	The entity shall: 1) map supply chain elements and identify any interdependency 2) identify and address any weaknesses or deficiencies during independent or organizational assessments of the mapped supply chain elements 3) establish a formal review/audit process 4) conduct regular assessments and audits of supply chain elements						

Implementation Guidance (for information purpose only)

Evidence generated during independent or organizational assessments of supply chain elements (e.g., penetration testing, audits, verification/validation activities) is documented and used in follow-on processes implemented by entities to respond to the risks related to the identified weaknesses and deficiencies. Supply chain elements include, for example, supplier development processes and supplier distribution systems.

T7.8.7	Supply of Critical Information System Components	Priority / Applicability				P4 / Based on risk assessment
Control	The entity shall ensure an adequate supply of critical information system and systems components.					
Sub-Control	The entity shall: 1) define contingency plan for any supply of critical information system component 2) stockpiling of critical spare components 3) use multiple suppliers for critical components					

Implementation Guidance (for information purpose only)

Adversaries can attempt to impede organizational operations by disrupting the supply of critical information system components or corrupting supplier operations. Controls to ensure adequate supplies of critical information system components include, for example:

a. the use of multiple suppliers throughout the supply chain for the identified critical components; and
b. stockpiling of spare components to ensure operation during mission-critical times.

T8 Information Security Incident Management

T8	Information Security Incident Management
Objective	To ensure that information security incidents are communicated in a manner allowing timely corrective actions to be taken.
Performance Indicator	Percentage of security incidents reported within the required timeframe and classified according to incident classification policy

T8.1	Information Security Incident Management Policy
Objective	To maintain an information security incident management policy covering the information security incident procedures covering the detection, reporting and treatment of incidents
Performance Indicator	Extent of information security incident management policy deployment and adoption across the entity
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Unsuitable or outdated information security incident management policy • Unawareness of information security incident management policy

T8.1.1	Information Security Incident Management Policy	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall establish a policy to manage and guide the response to information security incidents.		
Sub-Control	The incident management policy shall: 1) be appropriate to the purpose of the entity 2) include statement of the management commitment, purpose, objective and scope of the policy 3) outline roles and responsibilities 4) provide the framework for managing incidents 5) address sector and national level requirements for handling and reporting incidents 6) be documented and communicated to all users 7) be read and acknowledged formally by all users 8) be maintained, reviewed, exercised and updated at planned intervals or if significant changes occur		

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard (also refer to National Cyber Response Framework).

The information security incident management policy facilitates the implementation of the associated controls to ensure appropriate reaction to any actual or suspected security incidents relating to information assets. The policy can, for example, contain in addition to the required sub-controls:

a. Incident classification
b. Procedure for reporting information security events or weaknesses
c. Procedure for incident handling

The information systems acquisition, development and maintenance policy can be included as part of the general information security policy, in a single policy document, or can be represented by multiple policies reflecting the complex nature of certain entities.

T8.2	Management of Information Security Incidents and Improvements
Objective	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.
Performance Indicator	Percentage of security incidents that met reporting thresholds, were reported within specified timeframes, and were classified according to the incident classification policy.
Automation Guidance	Incident management and tracking solutions should be considered. They can be very helpful to support teamwork, in particular in large entities. They are also useful for trend analysis and to support management with analysis of threats and of incident impact.
Relevant Threats and Vulnerabilities	• Lack of incident response training • Inappropriate incident response testing procedures

T8.2.1	Incident Response Plan	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall develop a plan to guide incident response activities.		
Sub-Control	The entity shall develop an incident response plan encompassing the following: 1) processes and procedures for handling incidents before, during, and after an incident occurs to be documented, tested and maintained 2) communication plan to include internal and external parties 3) senior management approval of all plans and procedures 4) required resources and capabilities to be defined 5) establishment of a Computer Security Incident Response Team (see T8.2.2)		

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard (also refer to National Cyber Response Framework).

The entity should consider the following:

a. Develop an incident response plan that:
   1- Provides the entity with a roadmap for implementing its incident response capability;
   2- Describes the structure and organization of the incident response capability;
   3- Provides a high-level approach for how the incident response capability fits into the overall entity;
   4- Meets the unique requirements of the entity, which relate to mission, size, structure, and functions;
   5- Defines reportable incidents;
   6- Provides metrics for measuring the incident response capability within the entity;
   7- Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
   8- Is reviewed and approved by defined personnel or roles;

b. Make the incident response plan available to defined incident response personnel (identified by name and/or by role- and organizational elements;
c. Review and test the incident response plan in defined frequency;
d. Update the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
e. Communicate incident response plan changes to defined incident response personnel (identified by name and/or by role) and organizational elements; and
f. Protect the incident response plan from unauthorized disclosure and modification.

It is important that entities develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, entities consider the coordination and sharing of information with external entities, including, for example, external service providers and entities involved in the supply chain for organizational information systems.

T8.2.2	Computer Security Incident Response Team	Priority	P2
		Applicability	Based on risk assessment
Control	The entity shall establish a Computer Security Incident Response Team (CSIRT) in charge of the incident management and response plan.		
Sub-Control	The entity shall establish a CSIRT as follows: 1) Identify stakeholders and participants 2) Secure funding for CSIRT operations 3) Decide on the range and level of services the CSIRT will offer 4) Determine the CSIRT reporting structure, authority, and organizational model 5) Identify required resources such as staff, equipment, and infrastructure 6) Define interactions and interfaces 7) Define roles, responsibilities, and the corresponding authority 8) Document the workflow 9) Develop policies and corresponding procedures 10) Announce the CSIRT when it becomes operational to create the appropriate level of awareness		

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard (also refer to National Cyber Response Framework).

Entities should identify members in the entity to form the proper CSIRT. The establishment of the team should take place before developing the Incident Response plan. One of the CSIRT's responsibilities is to create the IR Plan.

Here are some of the CSIRT members:
- Team leader who is usually a senior manager whose responsibility is to take charge of incidents and direct actions to other team members
- Boundary protection experts. Normally individuals that are expert in firewalls, routers and IDSs that sits at the edge of the network.
- Network administrators

- Physical security members
- Human resources might be involved if the attach was originated by an employee
- Communication might be involved to become the public face for incidents that became public.

Here are some of the primary responsibilities of the CSIRT:

- Develop incident policy, plan, and procedures
- Response to incidents and minimizing the impact
- Investigate incidents and determine the cause
- prevent future incident by recommending security controls
- Handle incident reporting and communication to all stakeholder involved internally and externally
- Protect collected evidence

T8.2.3	Incident Classification	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity shall assess and classify information security incidents.					
Sub-Control	The entity shall: 1) establish an incident classification scheme in line with the incident response policy taking into account TRA's issuances with regard to incident management 2) assess and identify the incidents that should be reported at the sector and national level					
Implementation Guidance (for information purpose only)						

Classification and prioritization of incidents can help to identify the impact and extent of an incident. A point of contact should assess the information security events using the agreed information security event and incident classification scale and decide whether the events should be classified as information security incidents.

In case where the entity has CSIRT, the assessment and decision can be forwarded to the CSIRT for confirmation or reassessment. Results of the assessment and decision should be recorded in detail for the purpose of future reference and verification.

An attack is classified as an incident if the attack is directed against information assets, has a realistic chance of success and threatens the confidentiality, integrity and availability of information resources and assets.

An indication of an incident can be one or more of the following:

- if dormant or inactive accounts started accessing system resources, querying servers, or engaged in other activities
- if modification of logs occurs and the systems administrator cannot determine explicitly the authorized individual who modified them
- presence of hacking tools
- notifications by partner or peer
- notification by the attacker

T8.2.4	Incident Response Training	Priority	P4
		Applicability	Based on risk assessment
Control	The entity shall provide incident response training to information system users.		
Sub-Control	The entity shall: 1) establish a training program for the cyber security incident response team (CSIRT), in line with the Awareness and Training Policy (refer to M3.1.1) 2) ensure that the program covers all incident response procedures as well as their users		

Implementation Guidance (for information purpose only)

In designing the incident response training, entities should customize the content and level of details based on the targeted audience to allow attendees to focus on the information that is relevant to them.

As such, end users may only need to identify an incident or suspicious activities and call the right contact, system administrators may require technical training on how to handle/remediate incidents, and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration.

T8.2.5	Incident Response Testing	Priority	P4
		Applicability	Based on risk assessment
Control	The entity shall test its incident response capability.		
Sub-Control	The entity shall: 1) develop testing procedures and cases to validate effectiveness and usefulness of its incident response capability 2) establish expected test results 3) conduct incident response capability testing and compare outcome to the expected results to identify gaps and weaknesses for remediation		

Implementation Guidance (for information purpose only)

The entity should develop testing procedures to determine the overall effectiveness of its incident response capabilities and to identify potential weaknesses or deficiencies. Incident response testing must simulate pre-defined breach scenarios across the incident response lifecycle from including detection, reporting, and recovery to normal operations. Incident response testing includes, for example, the use of checklists, tabletop (discussion-based) exercises, and functional (performance of duties in a simulated environment) exercises. Entities should participate in sector, national, and international exercises to further test incident response capabilities.

T8.2.6	Incident Response Assistance	Priority / Applicability	P4 / Based on risk assessment
Control	The entity shall provide an incident response support resource to offer advice and assistance in case of an incident.		
Sub-Control	The entity shall: 1) assign the appropriate resources needed to support employees and external party in handling and reporting of security incidents; 2) establish and make available the procedure to get in touch with the assigned personnel		

Implementation Guidance (for information purpose only)

The entity should provide an incident response support resources as part of its incident response capability to provide advice and assistance to users of the information system during steady state operation and incidents for the detection, handling and reporting of security incidents.

The entity should provide an incident response support resources in different forms to reach the widest audience, such as:

- informative website
- online knowledge base
- call center, etc.

Moreover, the entity should coordinate with external providers (for example, national CERT) through its incident response capability for help in the detection and handling of incidents within the entity.

T8.2.7	Information Security Incident Documentation	Priority / Applicability	P4 / Based on risk assessment
Control	The entity shall document all information security incidents.		
Sub-Control	The entity shall: 1) identify the relevant data to be collected before, during and after an information security incident takes place 2) collect and document relevant data related to all security incidents 3) protect the information security incident documentation		

Implementation Guidance (for information purpose only)

Documenting information security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports

T8.2.8	Learning From Information Security Incidents	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity shall institutionalize the learning from information security incidents.					
Sub-Control	The entity shall: 1) establish detailed incident records including all related activities and outcomes where applicable 2) develop lessons learned and where applicable identify additional controls to avoid similar incidents in the future					

Implementation Guidance (for information purpose only)

There should be mechanisms in place to enable the types, volumes, costs, and impacts of information security incidents to be quantified and monitored. The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents and inform risk assessment and risk treatment activities.

Investigations based on information distributed by an information sharing community should be performed, to reduce the risks of similar incidents and develop a better understanding of the risks facing the community and any related significant information infrastructures. Such investigations could be performed by the community members involved, or by a supporting entity, if one exists.

Following reported incidents, post incident reviews should be performed by members of the information sharing community to trigger updates to security incident response plans, related procedures and the business risk profile, and implementation of additional controls even if the member was not affected by the incident in question. Each member should ensure that reported incident responses are assessed, and any lessons or possible improvements to the member's own processes are identified and acted upon to continuously improve its own response processes.

T8.2.9	Collection of Evidence	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity shall identify, collect, and preserve the information, which can serve as evidence.					
Sub-Control	The entity shall: 1) identify the requirements of the applicable jurisdictions 2) establish procedures for collecting evidence taking into account : - chain of custody - safety of evidence - safety of the personnel - roles and responsibilities of personnel involved - competency of the personnel - documentation - briefing - other identified requirements					

Implementation Guidance (for information purpose only)

Internal procedures should be developed and followed when dealing with evidence for the purposes of disciplinary and legal action.

Identification is the process involving the search for, recognition and documentation of potential evidence. Collection is the process of gathering the physical items that can contain potential evidence. Acquisition is the process of creating a copy of data within a defined set. Preservation is the process to maintain and safeguard the integrity and original condition of the potential evidence.

In general, the procedures for evidence should provide processes of identification, collection, acquisition and preservation in accordance with different types of media, devices and status of devices, e.g., powered on or off. The procedures should take account of:

a- chain of custody;
b- safety of evidence;
c- safety of the personnel;
d- roles and responsibilities of personnel involved;
e- competency of the personnel;
f- documentation;
g- briefing.

Where available, certification or other relevant means of qualification of personnel and tools should be sought, so as to strengthen the value of the preserved evidence.

Forensic evidence may transcend organizational or jurisdictional boundaries. In such cases, it should be ensured that the entity is entitled to collect the required information as forensic evidence. The requirements of different jurisdictions should also be considered to maximize chances of admission across the relevant jurisdictions.

T8.3	Information Security Events and Weaknesses Reporting
Objective	To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken
Performance Indicator	Percentage of information security incidents reported within the required time frame per applicable incident category as defined in the information security incident management policy
Automation Guidance	For an automated identification of weaknesses, a large number of vulnerability scanning tools are available. Some enterprises have also found commercial services using remotely managed scanning appliances to be effective. To help standardize the definitions of discovered vulnerabilities in multiple departments of an entity or even across entities, it is preferable to use vulnerability scanning tools that measure security flaws and map them to vulnerabilities and issues categorized using one or more of the following industry-recognized vulnerability, configuration, and platform classification schemes and languages: CVE, CCE, OVAL, CPE, CVSS, and/or XCCDF. Advanced vulnerability scanning tools can be configured with user credentials to log in to scanned systems and perform more comprehensive scans than can be achieved without login credentials. The frequency of scanning activities, however, should increase as the diversity of an entity's systems increases to account for the varying patch cycles of each vendor. Also, event log collectors and incident management systems should be considered. These technologies provide log collection, normalization, correlation and analysis: they can be very helpful both to detect incidents in their early stages and to investigate incidents.
Relevant Threats and Vulnerabilities	• Leakage of reported weaknesses • Unsuitable reporting procedures

T8.3.1	Situational Awareness	Priority				P4
		Applicability	Based on risk assessment			
Control	The entity shall develop a situational awareness culture by participating in the information sharing community and obtaining cyber security information from various sources.					
Sub-Control	The entity shall: 1) identify priority information and share it internally to build the entity context 2) for the sector context, identify and share priority information that is relevant to entities in the same sector to build the sector context 3) for the national context, identify and share priority information that is relevant across all sectors to build the national context					

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA relevant issuances, guidance, and activities in this regard (also refer to National Cyber Response Framework, and National Cyber Information Sharing Policy).

Priority information is information that may enable other community members to avoid or minimize similar undesirable events. It is important that such information is shared urgently, even if it is not fully analyzed or confirmed. The legal department, security vendors, third-party cyber threat intelligence providers, as well as the regulator should discuss what information can be shared and with whom.

T8.3.2	Reporting Information Security Events	Priority Applicability	P4 Based on risk assessment
Control	The entity shall report information security events through appropriate management channels.		
Sub-Control	The entity shall: 1) identify a designated event point of contact (e.g. CSIRT) 2) establish an information security events reporting procedure 3) establish an event communication and reporting approach to the appropriate stakeholder (including appropriate authority) 4) ensure the reporting approach accounts for all sector and national level management channels		

Implementation Guidance (for information purpose only)

All employees and external party users should be made aware of their responsibility to report any information security events as quickly as possible. They should also be aware of the procedure for reporting information security events and the point of contact (POC) where the events should be reported to.

Situations to be considered for information security event reporting include:

a. ineffective security control
b. breach of information integrity, confidentiality or availability expectations
c. human errors;
d. non-compliances with policies or guidelines;
e. breaches of physical security arrangements;
f. uncontrolled system changes;
g. malfunctions of software or hardware;
h. access violations.

T8.3.3	Reporting Security Weaknesses	Priority / Applicability				P4 / Based on risk assessment
Control	The entity shall report observed or suspected information security weaknesses in systems or services.					
Sub-Control	The entity shall: 1) establish and make available a procedure for employees and external third party users to report information security weaknesses as soon as identified 2) establish a CSIRT as a point of contact for any information security related issue 3) ensure that no user is trying to exploit the weakness					

Implementation Guidance (for information purpose only)

A security weakness (or vulnerability) is a flow which allows an attacker to reduce a system's information assurance.

All employees, contractors and external party users should report these matters to the point of contact as quickly as possible in order to prevent information security incidents. The reporting mechanism should be as easy, accessible and available as possible. They should be informed that they should not, in any circumstances, attempt to prove a suspected weakness. Testing weaknesses might be interpreted as a potential misuse of the system and could also cause damage to the information system or service and result in legal liability for the individual performing the testing.

T9 Information Systems Continuity Management

T9	Information Systems Continuity Management
Objective	To ensure business continuity and protection of critical information
Performance Indicator	Percentage of information assets with measured availability above the minimum acceptable thresholds

T9.1	Information Systems Continuity Management Policy
Objective	To maintain an information continuity management policy covering the continuity and redundancy of information based on their level of criticality
Performance Indicator	Percentage of organizational units with an established information continuity plan in accordance with the information continuity management policy
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Unsuitable information systems continuity management policy • Unawareness of information systems continuity management policy among IT staff

T9.1.1	Information Systems Continuity Planning Policy	Priority					P4
		Applicability	Based on risk assessment				
Control	The entity shall establish an information systems continuity planning policy.						
Sub-Control	The information systems continuity planning policy shall: 1) be appropriate to the purpose of the entity 2) include statement of the management commitment, purpose, objective and scope of the policy 3) outline roles and responsibilities 4) provide the framework for continuity of information in adverse situations in accordance with the entity overall business continuity and / or disaster recovery planning 5) be documented and communicated to all users 6) be read and acknowledged formally by all users 7) be maintained, reviewed, tested and updated at planned intervals or if significant changes occur						

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard.

An entity should determine whether the continuity of information security is captured within the BCM process or within the (IT) disaster recovery management (DRM- process. Information security requirements should be determined when planning for business continuity and disaster recovery.

In the absence of formal business continuity and disaster recovery planning, information security management should assume that information security requirements remain the same in adverse situations, compared to normal operational conditions. Alternatively, an organization could perform a business impact analysis (BIA- for information security aspects to determine the information security requirements applicable to adverse situations.

The process of including information security in the business continuity management should bring together the following key elements of business continuity management:

a. understanding the risks the entity is facing in terms of likelihood and impact in time, including an identification and prioritization of critical business processes;
b. identifying all the assets involved in critical business processes;
c. understanding the impact which interruptions caused by information security incidents are likely to have on the business (it is important that solutions are found that will handle incidents causing smaller impact, as well as serious incidents that could threaten the viability of the entity), and establishing the business objectives of information systems;
d. considering the purchase of suitable insurance which may form part of the overall business continuity process, as well as being part of operational risk management;
e. identifying and considering the implementation of additional preventive and mitigating controls;
f. identifying sufficient financial, organizational, technical, and environmental resources to address the identified information security requirements;
g. ensuring the safety of personnel and the protection of information systems and organizational property;

The process should bring together the following key elements of business continuity management:

a. formulating and documenting business continuity plans addressing information security requirements in line with the agreed business continuity strategy;
b. regular testing and updating of the plans and processes put in place;
c. ensuring that the management of business continuity is incorporated in the entity's processes and structure; responsibility for the business continuity management process should be assigned at an appropriate level within the entity.

T9.2	Information Security Aspects of Information Continuity Management
Objective	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption
Performance Indicator	Percentage of organizational units with information continuity plans that have been adequately documented and proven by suitable testing
Automation Guidance	Not applicable
Relevant Threats and Vulnerabilities	• Destruction of equipment or media • Corruption of data

T9.2.1	Developing Information Systems Continuity Plans	Priority				P3	
		Applicability	Based on risk assessment				
Control	The entity shall develop its information systems continuity plans.						
Sub-Control	The entity shall: 1) identify information continuity requirements in line with the entity's overall business continuity planning and / or disaster recovery 2) specify the escalations criteria and the conditions for its activation 3) outline information continuity roles and responsibilities, and assign individuals with contact information 4) define a safe mode when incidents are detected that restrict the entity's operation in accordance with the information systems continuity policy						

Implementation Guidance (for information purpose only)

Critical entities shall also take into account any other TRA's relevant issuances, guidance, and activities in this regard.

The continuity planning process should consider the following:
a. identification and agreement of all responsibilities and continuity procedures;
b. identification of the acceptable loss of information and services;
c. implementation of the procedures to allow recovery and restoration of business operations and availability of information in required time-scales; particular attention needs to be given to the assessment of internal and external business dependencies and the contracts in place;
d. operational procedures to follow pending completion of recovery and restoration;
e. documentation of agreed procedures and processes;
f. appropriate education of staff in the agreed procedures and processes, including crisis management;
g. testing and updating of the plans.

The planning process should focus on the required business objectives, e.g. restoring of specific communication services to customers in an acceptable amount of time. The services and resources facilitating this should be identified, including staffing, non-information processing resources, as well as fallback arrangements for information systems. Such fallback arrangements may include arrangements with third parties in the form of reciprocal agreements, or commercial subscription services.

If alternative temporary locations are used, the level of implemented security controls at these locations should be equivalent to the main site.

T9.2.2	Implementing Information Systems Continuity Plans	Priority				P3	
		Applicability	Based on risk assessment				
Control	The entity shall implement for the established information security plans.						
Sub-Control	The entity shall: 1) establish information systems continuity capabilities based on the established plans						

Implementation Guidance (for information purpose only)

An entity should ensure that:

a. an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence;
b. incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security is nominated;
c. documented plans, response and recovery procedures are developed and approved, detailing how the entity will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security (continuity) objectives.

According to the information security continuity requirements, the entity should establish, document, implement and maintain:

a. information security controls within business continuity and/or disaster recovery processes, procedures and supporting (information- systems and tools;
b. processes, procedures and implementation changes to maintain existing information security controls during an adverse situation;
c. compensating controls for information security controls that cannot be maintained during an adverse situation.

T9.3	Testing, Maintaining and Reassessing Plans
Objective	To ensure the effectiveness of the information systems continuity management plans and they are always up-to-date
Performance Indicator	Percentage of information systems that went through an annual testing
Automation Guidance	An automated solution to plan tests and to keep track of the results and the improvement areas should be considered.
Relevant Threats and Vulnerabilities	• Unperformed information systems continuity management testing • Outdated information systems continuity management plan

T9.3.1	Testing, Maintaining and Re-Assessing Information Systems Continuity Plans	Priority				P3	
		Applicability	Based on risk assessment				
Control	The entity shall test, maintain and re-assess its information systems continuity plans.						
Sub-Control	The entity shall: 1) periodically test the continuity plan for the information systems following the established procedures to determine the effectiveness of the plan and the organizational readiness to execute the plan 2) establish lessons learned and update the information systems continuity plans to ensure they are always up-to-date						

Implementation Guidance (for information purpose only)

Business continuity plan tests should ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked.

The test schedule for business continuity plan(s) should indicate how and when each element of the plan should be tested. Each element of the plan(s) should be tested frequently.
A variety of techniques should be used in order to provide assurance that the plan(s) will operate in real life. These should include:

a. table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions);
b. simulations (particularly for training people in their post-incident/crisis management roles);
c. technical recovery testing (ensuring information systems can be restored effectively);
d. testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site);
e. tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment);
f. complete rehearsals (testing that the entity, personnel, equipment, facilities, and processes can cope with interruptions).

These techniques can be used by any entity. They should be applied in a way that is relevant to the specific recovery plan. The results of tests should be recorded and actions taken to improve the plans, where necessary.

Responsibility should be assigned for regular reviews of each business continuity plan. The identification of changes in business arrangements not yet reflected in the business continuity plans should be followed by an appropriate update of the plan. This formal change control process should ensure that the updated plans are distributed and reinforced by regular reviews of the complete plan.

Examples of changes where updating of business continuity plans should be considered are acquisition of new equipment, upgrading of systems and changes in:

- personnel;
- addresses or telephone numbers;
- business strategy;
- location, facilities, and resources;
- legislation;
- contractors, suppliers, and key customers;
- processes, or new or withdrawn ones;
- risk (operational and financial)

Most of this information is derived from a variety of sources, including:

- ISO/IEC 27001:2005 "Information technology — Security techniques — Information security management systems — Requirements"
- ISO/IEC 27002:2005 "Information technology — Security techniques — Code of practice for Information security management"
- ISO/IEC 27005:2005 "Information technology — Security techniques —Information security risk management"
- ISO/IEC 27010:2012 "Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications"
- ISO/IEC 27032:2012 "Information technology — Security techniques — Guidelines for cybersecurity"
- NIST Special Publication 800-53 Revision 4 "Security and Privacy Controls for Federal Information Systems and Organizations"
- Abu Dhabi Information Security Standards Version 1 and Version 2, developed by Abu Dhabi Systems and Information Centre (ADSIC)
- SANS 20 Critical Security Controls for Effective Cyber Defense Version 4.1

Annex A: Summary of Always Applicable Controls

The following table provides a list of "Always Applicable" security controls. As a recap, "Always Applicable" security controls represent critical requirements for building foundational IA capabilities and must be implemented by each relevant entity regardless of its risk assessment outcomes. Omission of any of these security controls constitutes non-conformity to this Regulation.

Overall, a total of 34 management controls constitute the list of "Always Applicable" controls as outlined in Table 5 below.

Table 5: Summary of Always Applicable Controls

Control Number	Control Name
M1 – Strategy and Planning	
M1.1 - Entity Context and Leadership	
M1.1.1	Understanding the Entity and its Context
M1.1.2	Leadership and Management Commitment
M1.1.3	Roles and Responsibilities for Information Security
M1.2 - Information Security Policy	
M1.2.1	Information Security Policy
M1.2.2	Supporting Policies for Information Security
M1.4 - Support	
M1.4.1	Resources
M1.4.2	Internal and External Communication
M1.4.3	Documentation
M2 - Information Security Risk Management	
M2.1 - Information Security Risk Management Policy	
M2.1.1	Information Security Risk Management Policy
M2.2 – Information Security Risk Assessment	
M2.2.1	Information Security Risk Identification
M2.2.2	Information Security Risk Analysis
M2.2.3	Information Security Risk Evaluation

Control Number	Control Name
M2.3 - Information Security Risk Treatment	
M2.3.1	Information Security Risk Treatment Options
M2.3.2	Identification of Controls
M2.3.3	Risk Treatment Plan
M2.3.4	Statement of Applicability
M2.3.5	Information Security Objectives
M2.4 - Ongoing Information Security Risk Management	
M2.4.1	Risk Monitoring and Review
M2.4.2	Risk Communication and Consultation
M3 – Awareness and Training	
M3.2 – Awareness and Training Planning	
M3.2.1	Awareness and Training Program
M3.3 – Security Training	
M3.3.1	Training Needs
M3.3.2	Implementation Plan
M3.3.3	Training Execution
M4 - Human Resources Security	
M4.1 - Human Resources Security Policy	
M4.1.1	Human Resources Security Policy
M4.2 – Prior to Employment	
M4.2.1	Screening
M4.2.2	Terms and Conditions of Employment
M4.2 – Prior to Employment	
M4.3.1	Management Responsibilities
M4.3.2	Disciplinary Process

Control Number	Control Name
M4.4 – Termination or Change of Employment	
M4.4.1	Termination Responsibilities
M4.4.2	Return of Assets
M4.4.3	Removal of Access Rights
M6 - Performance Evaluation and Improvement	
M6.2 - Performance Evaluation	
M6.2.1	Monitoring, Measurement, Analysis and Evaluation
M6.2.2	Internal Audits
M6.3 – Improvement	
M6.3.1	Corrective Action
M6.3.2	Continual Improvement

Annex B: Summary of the Prioritized Controls

The following table provides a list of the prioritized security controls. As a recap, the concept of "Prioritization" relates to grouping the security controls in order of importance for realizing a minimum level of information assurance protection, and for enabling a phased and incremental implementation of this Regulation.

Overall, the distribution of security controls across the four priority levels is outlined in Table 6, and the detailed listing is provided in Table 7, below.

Table 6: Distribution of Security Controls across Priority Levels

Control Number	Control Name
P1	39
P2	69
P3	35
P4	45

Table 7: Summery of prioritize controls

Control #	Control Name	Control #	Control Name
P1 Controls			
M1.1.1	Understanding the Entity and its Context	T1.4.1	Management of Removable Media
M1.1.2	Leadership and Management Commitment	T3.4.1	Controls Against Malware
M1.1.3	Roles and Responsibilities for Information Security	T3.5.1	Information Backup
M1.2.1	nformation Security Policy	T3.6.3	Monitoring System Use
M1.3.5	Identification of Risks Related to External Parties	T4.5.1	Network Controls
M1.4.1	Resources	T4.5.3	Segregation in Networks
M2.1.1	Information Security Risk Management Policy	T5.2.1	User Registration
M2.2.1	Information Security Risk Identification	T5.2.2	Privilege Management
M2.2.2	Information Security Risk Analysis	T5.2.3	User Security Credentials Management
M2.2.3	Information Security Risk Evaluation	T5.2.4	Review of User Access Rights
M2.3.1	Information Security Risk Treatment Options	T5.3.1	Use of Security Credentials
M2.3.2	Identification of Controls	T5.4.2	User Authentication for External Connections
M2.3.3	Risk Treatment Plan	T5.4.3	Equipment Identification in Networks
M2.3.4	Statement of Applicability	T5.4.5	Network Connection Control
M2.4.1	Risk Monitoring and Review	T5.5.1	Secure Log-On Procedures
M2.4.2	Risk Communication and Consultation	T5.5.2	User Identification and Authentication
M3.3.1	Training Needs	T5.5.3	User Credentials Management system
M4.4.1	Termination Responsibilities	T5.6.1	Information Access Restriction
M4.4.2	Return of Assets	T7.7.1	Control of Technical Vulnerabilities
M4.4.3	Removal of Access Rights		

Control #	Control Name	Control #	Control Name
P2 Controls			
M1.2.2	Supporting Policies for Information Security	T2.2.2	Physical Entry Controls
M1.3.1	Authorization Process for Information Systems	T2.2.3	Securing Offices, Rooms and Facilities
M1.3.2	Confidentiality Agreements	T2.3.1	Equipment Siting and Protection
M1.3.6	Addressing Security When Dealing with Customers	T2.3.8	Unattended User Equipment
M1.3.7	Addressing Security in Third Party	T3.2.1	Common Systems Configuration Guidelines
M1.4.2	Agreements	T3.2.4	Segregation of Duties
M1.4.3	Internal and External Communication	T3.2.5	Separation of Development, Test and Operational Facilities
M2.3.5	Documentation	T3.6.2	Audit Logging
M3.1.1	Information Security Objectives	T3.6.4	Protection of Log Information
M3.2.1	Awareness and Training Policy	T3.6.5	Administrator and Operator Logs
M3.3.3	Awareness and Training Program	T4.2.1	Information Transfer Procedures
M3.3.4	Training Execution	T4.3.1	Electronic Commerce
M3.3.5	Training Results	T4.5.2	Security of Network Services
M3.4.1	Records Documentation	T4.5.4	Security of Wireless Networks
M4.1.1	Awareness Campaign	T5.1.1	Access Control Policy
M4.2.1	Human Resources Security Policy	T5.4.1	Policy on Use of Network Services
M4.2.2	Screening Terms and Conditions of Employment	T5.4.7	Wireless Access
M4.3.1	Management Responsibilities	T5.6.2	Sensitive System Isolation
M4.3.2	Disciplinary Process	T6.2.1	Service Delivery
M5.1.1	Compliance Policy	T6.2.2	Monitoring and Review of Third Party Services
M5.2.1	Identification of Applicable Legislation	T6.2.3	Managing Changes to Third Party Services
M5.2.3	Protection of Organizational Records	T6.3.1	Information Security Requirements for Cloud Environments
M5.2.6	Regulation of Cryptographic Controls	T6.3.2	Service Delivery Agreements with Cloud Providers
M5.4.1	Technical Compliance Checking	T7.3.1	Input Data Validation

Control #	Control Name	Control #	Control Name
M6.2.1	Monitoring, Measurement, Analysis and Evaluation	T7.3.2	Control of Internal Processing
M6.2.2	Internal Audits	T7.3.3	Message Integrity
M6.3.1	Corrective Action	T7.3.4	Output Data Validation
M6.3.2	Continual Improvement	T7.4.1	Policy on the Use of Cryptographic Controls
T1.1.1	Asset Management Policy	T7.4.2	Key Management
T1.2.1	Inventory of Assets	T7.6.3	Restrictions on Changes to Software Packages
T1.2.2	Ownership of Assets	T7.6.4	Information Leakage
T1.2.3	Acceptable Use of Assets	T 8.1.1	Information Security Incident Management Policy
T1.2.4	Acceptable Bring Your Own Device (BYOD) Arrangements	T8.2.1	Incident Response Plan
T1.4.2	Disposal of Media	T8.2.2	Computer Security Incident Response Team
T2.2.1	Physical Security Perimeter		
P3 Controls			
M3.3.2	Implementation Plan	T4.1.1	Communications Policy
M5.2.4	Data Protection and Privacy of Personal Information	T4.2.2	Agreements on Information Transfer
M5.2.5	Prevention of Misuse of Information Systems	T4.2.3	Physical Media in Transit
M6.1.1	Performance Evaluation Policy	T4.2.4	Electronic Messaging
T1.3.1	Classification of Information	T4.3.2	On-Line Transactions
T1.3.2	Labeling of Information	T5.4.6	Network Routing Control
T1.3.3	Handling of Information Assets	T5.6.3	Publicly Accessible Content
T2.2.5	Working in Secure Areas	T7.2.1	Security Requirements Analysis and Specification
T2.2.6	Public Access, Delivery, and Loading Areas	T7.5.2	Protection of System Test Data
T2.3.4	Equipment Maintenance	T7.5.3	Access Control to Program Source Code
T2.3.5	Security of Equipment Off-Premises	T7.6.1	Change Control Procedures
T2.3.6	Secure Disposal or Re-Use of Equipment	T7.6.2	Technical Review of Applications After Operating System Changes
T2.3.7	Removal of Property	T7.6.5	Outsourced Software Development

Control #	Control Name	Control #	Control Name
P3 Controls			
T2.3.9	Clear Desk and Clear Screen Policy	T7.8.6	Processes to Address Weaknesses or Deficiencies
T3.2.2	Documented Operating Procedures	T9.2.1	Developing Information Systems Continuity Plans
T3.3.2	System Acceptance and Testing	T9.2.2	Implementing Information Systems Continuity Plans
T3.6.1	Monitoring Policy and Procedures	T9.3.1	Testing, Maintaining and Re-Assessing Information Systems Continuity Plans
T3.6.6	Fault Logging		
P4 Controls			
M1.3.3	Contact with Authorities	T5.7.2	Teleworking
M1.3.4	Contact with Special Interest Groups	T6.1.1	Third Party Security Policy
M5.2.2	Intellectual Property Rights (IPR)	T7.1.1	Information Systems Acquisition, Development and Maintenance Policy
M5.2.7	Liability to the Information Sharing Community	T7.2.2	Developer-Provided Training
M5.3.1	Compliance with Security Policies and Standards	T7.5.1	Control of Operational Software
M5.5.1	Information Systems Audit Controls	T7.8.1	Supply Chain Protection Strategy
M5.5.2	Protection of Information Systems Audit Tools	T7.8.2	Supplier Reviews
M5.5.3	Audit of Community Functions	T7.8.3	Limitation of Harm
T2.1.1	Physical and Environmental Security Policy	T7.8.4	Supply Chain Operations Security
T2.2.4	Protecting Against External and Environmental Threats	T7.8.5	Reliable Delivery
T2.3.2	Supporting Utilities	T7.8.7	Supply of Critical Information System Components
T2.3.3	Cabling Security	T8.2.3	Incident Classification
T3.1.1	Operations Management Policy	T8.2.4	Incident Response Training
T3.2.3	Change Management	T8.2.5	Incident Response Testing
T3.3.1	Capacity Management	T8.2.6	Incident Response Assistance
T3.6.7	Clock Synchronization	T8.2.7	Information Security Incident
T4.2.5	Business Information Systems	T8.2.8	Documentation
T4.3.3	Publicly Available Information	T8.2.9	Learning From Information Security Incidents

Control #	Control Name	Control #	Control Name
P4 Controls			
T4.4.1	Connectivity to Information Sharing Platforms	T8.3.1	Collection of Evidence
T4.4.2	Information Released into Information Sharing Communities	T8.3.2	Situational Awareness
T5.4.4	Remote Diagnostic and Configuration Protection	T8.3.3	Reporting Information Security Events
T5.5.4	Use of System Utilities	T9.1.1	Reporting Security Weaknesses
T5.7.1	Access Control for Mobile Devices		Information Systems Continuity Planning Policy

Annex C: Mapping of Controls against Leading Standards

The following table provides a list of the UAE IA Regulation security controls mapping against the security controls of ISO 27001, NIST Special Publication 800-53, SANS 20 and ADSIC Information Security Standards. This mapping enables the implementing entities to compare the requirements of the UAE IA Regulation against other leading standards.

Table 8: Mapping of UAE IA Regulation Controls against Leading Standards

Control Number	Control Name	ISO 27001 ISO 27002	NIST SP800 – 53r4	ADSIC v1.0	ADSIC v2.0
M1.1.1	Understanding the Entity and its Context	NONE	NONE	NONE	NONE
M1.1.2	Leadership and Management Commitment	A5.1.1, A.6.1.2	XX-1 controls, PM-1, IR-4, PL-2, CP-2, CP-4, IR-4, PL-1, PL-6, PM-2, SA-2; SP 800-39, SP 800-37	1.2.1	NONE
M1.1.3	Roles and Responsibilities for Information Security	A6.1.3	XX-1 controls, AC-5, AC-6, CM-9. PM-2; SP 800-39, SP 800-37	1.2.1	NONE
M1.2.1	Information Security Policy	A.5.1.1	XX-1 Controls, PM-1	2.1.1, 2.1.2	SG.8
M1.2.2	Supporting Policies for Information Security	NONE	XX-1 controls, CA-2, CA-7, RA-5, AU-1, AU-2, SI-4, AU-9	NONE	SG.8
M1.3.1	Authorization Process for Information Systems	A.6.1.4	PM-10, CA-1, CA-6; SP 800-37	3.3.1	IS.13

Control Number	Control Name	ISO 27001 ISO 27002	NIST SP800 – 53r4	ADSIC v1.0	ADSIC v2.0
M1.3.2	Confidentiality Agreements	A.6.1.5	PL-4, PS-6, SA-9	8.1.1	HR.1
M1.3.3	Contact Wwith Authorities	A.6.1.6	IR-4, IR-6, IR-7, PE-13, SA-19, SI-5	13.1.1	IM.5
M1.3.4	Contact Wwith Special Interest Groups	A.6.1.7	PM-15, SI-5	13.2.2	TA.5
M1.3.5	Identification of Risks Related to External Parties	A.6.2.1	PM-9, AC-20, CA-3, RA-3, SA-9	NONE	RM.2
M1.3.6	Addressing Security When Dealing Wwith Customers	A.6.2.2	AC-8 , AT-2, AT-3, CA-2, CA-3, PL-4, SA-9	NONE	NONE
M1.3.7	Addressing Security in Third Party Agreements	A.6.2.3	CA-3, PL-4, PS-6, PS-7, SA-9	NONE	TP.2
M1.4.1	Resources	5.2.1, A.6.1.2, A.10.3.1	XX-1 controls, PM-1, PM-2, CP-2, CP-4, IR-4, PL-1, PL-2, SA-2	NONE	SG.1.9
M1.4.2	Internal and External Communication	NONE	NONE	5.1.1, 5.1.2, 5.2.1, 5.2.2	TA.3, TA.6
M1.4.3	Documentation	4.3	NONE	NONE	NONE
M2.1.1	Information Security Risk Management Policy	NONE	RA-1, PM-9	None	NONE
M2.2.1	Information Security Risk Identification	4.2.1	RA-2	1.3.1	RM.2
M2.2.2	Information Security Risk Analysis	4.2.1	RA-3	3.1.1	RM.3
M2.2.3	Information Security Risk Evaluation	4.2.1	NONE	3.1.1	RM.3
M2.3.1	Information Security Risk Treatment Options	4.2.1	NONE	RM-3.1.2	RM.4
M2.3.2	Identification of Controls	4.2.1	NONE	NONE	RM.4
M2.3.3	Risk Treatment Plan	4.2.1	NONE	NONE	RM.4
M2.3.4	Statement of Applicability	4.2.1	NONE	3.3	NONE
M2.3.5	Information Security Objectives	NONE	NONE	NONE	NONE
M2.4.1	Information Security Risk Assessment Review and Update	4.2.3	RA-3	NONE	NONE

Control Number	Control Name	ISO 27001 ISO 27002	NIST SP800 – 53r4	ADSIC v1.0	ADSIC v2.0
M2.4.2	Risk Communication and Consultation	NONE	NONE	-	RM.2.2
M3.1.1	Awareness and Training Policy	NONE	AT-1	NONE	NONE
M3.2.1	Awareness and Training Program	5.2.2	NONE	4.2.1	TA.4
M3.3.1	Training Needs	5.2.2	NONE	4.2.1	TA.4
M3.3.2	Implementation Plan	NONE	NONE	4.2.1	TA.4
M3.3.3	Training Execution	5.2.2	AT-3	4.2.2	TA.4
M3.3.4	Training Results	NONE	NONE	NONE	NONE
M3.3.5	Records Documentation	5.2.2	AT-4	4.2.3	TA.4
M3.4.1	Awareness Campaign	NONE	AT-2	4.1.1, 4.1.1	TA.2
M4.1.1	Human Resources Security Policy	NONE	NONE	NONE	NONE
M4.2.1	Screening	A.8.1.2	PS-3	8.1.2	HR.2
M4.2.2	Terms and Conditions of Employment	A.8.1.3	AC-20, PL-4, PS-6, PS-7	8.1.3	HR.3
M4.3.1	Management Responsibilities	A.8.2.1	PL-4, PS-6, PS-7, SA-9	8.2.1	HR.1
M4.3.2	Disciplinary Process	A.8.2.3	PS-8	8.2.2	HR.5
M4.4.1	Termination Responsibilities	A.8.3.1	PS-4, PS-5	8.3.1	HR.6
M4.4.2	Return of Assets	A.8.3.2	PS-4, PS-5	8.3.2	HR.6
M4.4.3	Removal of Access Rights	A.8.3.3	AC-2, PS-4, PS-5	8.3.3	HR.6
M5.1.1	Compliance Policy	NONE	NONE	NONE	NONE
M5.2.1	Identification of Applicable Legislation	A.15.1.1	XX-1 controls, IA-7	1.3.3	SG.5
M5.2.2	Intellectual Property Rights (IPR)	A.15.1.2	SA-6	1.3.3	SG.5
M5.2.3	Protection of Organizational Records	A.15.1.3	AU-9, AU-11, CP-9, MP-1, MP-4, SA-5, SI-12	1.3.3	SG.5
M5.2.4	Data Protection and Privacy of Personal Information	A.15.1.4	PL-5; SI-12	1.3.3	SG.5

Control Number	Control Name	ISO 27001 ISO 27002	NIST SP800 – 53r4	ADSIC v1.0	ADSIC v2.0
M5.2.5	Prevention of Misuse of Information Systems	A.15.1.5	AC-8, AU-6, PL-4, PS-6, PS-8, SA-7	11.5.1	NONE
M5.2.6	Regulation of Cryptographic Controls	A.15.1.6	IA-7, SC-13	12.3.1	IS.5
M5.2.7	Liability to the Information Sharing Community	NONE	NONE	NONE	NONE
M5.3.1	Compliance with Security Policies and Standards	A.15.2.1	XX-1 controls, AC-2, CA-2, CA-7, IA-7, PE-8, SI-12	1.3.4, 2.0, 3.4.1, 6.2.1, 6.2.2, 6.2.3, 6.3.1, 6.3.2, 6.3.3	IS.1, SG.1, SG.8, SG.9, SG.10
M5.4.1	Technical Compliance Checking	A.15.2.2	CA-2, CA-7, RA-5	3.2.1, 3.4.1, 6.3.1, 6.3.2, 6.3.3	IS.13, SG.9, SG.10
M5.5.1	Information Systems Audit Controls	A.15.3.1	AU-1, AU-2, PL-6	NONE	SG.10
M5.5.2	Protection of Information Systems Audit Tools	A.15.3.2	AU-9	11.5.4	OM.13
M5.5.3	Audit of Community Functions	NONE	NONE	NONE	NONE
M6.1.1	Performance Evaluation Policy	NONE	NONE	NONE	NONE
M6.2.1	Monitoring, Measurement, Analysis and Evaluation	4.2.2 d)	PM-6	6.2.2, 6.2.3	SG.9
M6.2.2	Internal Audits	6, A.6.1.8	CA-2, CA-7; SP 800-39, SP 800-37	3.2.1	IS.13, SG.10
M6.3.1	Corrective Action	8.1	NONE	NONE	SG.1
M6.3.2	Continual Improvement	8.2	NONE	6.2.3	SG.1, SG.10
T1.1.1	Asset Management Policy	NONE	NONE	NONE	NONE
T1.2.1	Inventory of Assets	A.7.1.1	CM-8, CM-9, PM-5	7.1.1	AM.1
T1.2.2	Ownership of Assets	A.7.1.2	CM-8, CM-9, PM-5	7.1.2	AM.2
T1.2.3	Acceptable Use of Assets	A.7.1.3	AC-20, PL-4	7.1.3	HR.3
T1.2.4	Acceptable Bring Your Own Device (BYOD) Arrangements	NONE	NONE	NONE	NONE

Control Number	Control Name	ISO 27001 ISO 27002	NIST SP800 – 53r4	ADSIC v1.0	ADSIC v2.0
T1.3.1	Classification of Information	A.7.2.1	RA-2	7.2.1	AM.3
T1.3.2	Labeling of Information	A.7.2.2	AC-16, MP-2, MP-3, SC-16	7.2.2	AM.4
T1.3.3	Handling of Information Assets	A.7.2.2	AC-16, MP-2, MP-3, SC-16	7.2.2	AM.4
T1.4.1	Management of Removable Media	A.10.7.1	MP Family, PE-16	10.7.1	OM.16
T1.4.2	Disposal of Media	A.10.7.2	MP-6	10.7.2	OM.16
T2.1.1	Physical and Environmental Security Policy	NONE	PE-1	NONE	NONE
T2.2.1	Physical Security Perimeter	A.9.1.1	PE-3	9.1.1	PE.2
T2.2.2	Physical Entry Controls	A.9.1.2	PE-3, PE-5, PE-6, PE-7	9.1.2, 9.1.3	PE.2
T2.2.3	Securing Offices, Rooms and Facilities	A.9.1.3	PE-3, PE-4, PE-5	9.1.4	PE.2
T2.2.4	Protecting Against External and Environmental Threats	A.9.1.4	CP Family; PE-1, PE-9, PE-10, PE-11, PE-13, PE-15	9.1.5	PE.2
T2.2.5	Working in Secure Areas	A.9.1.5	AT-2, AT-3 , PL-4, PS-6, PE-2, PE-3, PE-4, PE-6, PE-7, PE-8	9.1.6	PE.3
T2.2.6	Public Access, Delivery, and Loading Areas	A.9.1.6	PE-3 , PE-7, PE-16	9.1.7	PE.2
T2.3.1	Equipment Siting and Protection	A.9.2.1	PE-1, PE-18	9.2.1	PE.2
T2.3.2	Supporting Utilities	A.9.2.2	PE-1, PE-9, PE-11, PE-12, PE-14	9.2.2	PE.2
T2.3.3	Cabling Security	A.9.2.3	PE-4, PE-9	9.2.3	NONE
T2.3.4	Equipment Maintenance	A.9.2.4	MA Family	9.2.4	OM.21
T2.3.5	Security of Equipment Off-Premises	A.9.2.5	MP-5, PE-17	9.2.5	PE.2
T2.3.6	Secure Disposal or Re-Use of Equipment	A.9.2.6	MP-6	9.2.6	OM.22
T2.3.7	Removal of Property	A.9.2.7	MP-5, PE-16	9.2.7	PE.2

Control Number	Control Name	ISO 27001 ISO 27002	NIST SP800 – 53r4	ADSIC v1.0	ADSIC v2.0
T2.3.8	Unattended User Equipment	A.11.3.2	AC-11, IA-2, PE-3, PE-5, PE-18, SC-10	11.3.2	PE.3
T2.3.9	Clear Desk and Clear Screen Policy	A.11.3.3	AC-11	11.3.3	PE.3
T3.1.1	Operations Management Policy	NONE	CM-1	10.1.1	NONE
T3.2.1	Common Systems Configuration Guidelines	NONE	CM-6	12.1.2	IS.3
T3.2.2	Documented Operating Procedures	A.10.1.1	XX-1 controls, CM-9	10.1.1	OM.1
T3.2.3	Change Management	A.10.1.2	CM-1, CM-3, CM-4, CM-5, CM-9	10.1.2	OM.2
T3.2.4	Segregation of Duties	A.10.1.3	AC-5	10.1.3	HR.4
T3.2.5	Separation of Development, Test and Operational Facilities	A.10.1.4	CM-2	10.1.4	OM.3
T3.3.1	Capacity Management	A.10.3.1	AU-4, AU-5, CP-2, SA-2, SC-5	10.3.1	IS.2
T3.3.2	System Acceptance and Testing	A.10.3.2	CA-2, CA-6, CM-3, CM-4, CM-9, SA-11	10.3.2	OM.4
T3.4.1	Controls Against Malware	A.10.4.1	AC-19, AT-2, SA-8, SC-2, SC-3, SC-7, SC-14, SI-3, SI-7	10.4.1	OM.6
T3.5.1	Information Backup	A.10.5.1	CP-9	10.5.1	OM.8
T3.6.1	Monitoring Policy and Procedures	NONE	AU -1	10.10.1	OM.5
T3.6.2	Audit Logging	A.10.10.1	AU-1, AU-2, AU-3, AU-4, AU-5, AU-8, AU-11, AU-12	10.10.2	OM.20
T3.6.3	Monitoring System Use	A.10.10.2	AU-1, AU-6, AU-7, PE-6, PE-8, SC-7, SI-4	10.10.3	OM.20
T3.6.4	Protection of Log Information	A.10.10.3	AU-9	10.10.4	OM.20
T3.6.5	Administrator and Operator Logs	A.10.10.4	AU-2, AU-12	10.10.5	OM.20
T3.6.6	Fault Logging	A.10.10.5	AU-2, AU-6, AU-12, SI-2	10.10.6	OM.20

Control Number	Control Name	ISO 27001 ISO 27002	NIST SP800 – 53r4	ADSIC v1.0	ADSIC v2.0
T3.6.7	Clock Synchronization	A.10.10.6	AU-8	10.10.7	OM.20
T4.1.1	Communications Policy	NONE	SC-1	10.8.1	SG.6
T4.2.1	Information Transfer Procedures	A.10.8.1	AC-1, AC-3, AC-4, AC-17, AC-18, AC-20, CA-3, PL-4, PS-6, SC-7, SC-16, SI-9	10.8.1	SG.6
T4.2.2	Agreements on Information Transfer	A.10.8.2	CA-3, SA-9	10.8.2	SG.6
T4.2.3	Physical Media in Transit	A.10.8.3	MP-5	10.8.3	OM.19
T4.2.4	Electronic Messaging	A.10.8.4	Multiple controls; electronic messaging not addressed separately in SP 800-53	10.8.4	OM.14
T4.2.5	Business Information Systems	A.10.8.5	CA-1, CA-3	10.8.5	NONE
T4.3.1	Electronic Commerce	A.10.9.1	AU-10, IA-8, SC-7, SC-8, SC-9, SC-3, SC-14	10.9.1	NONE
T4.3.2	On-Line Transactions	A.10.9.2	SC-3, SC-7, SC-8, SC-9, SC-14	10.9.2	NONE
T4.3.3	Publicly Available Information	A.10.9.3	SC-14	10.9.3	NONE
T4.4.1	Connectivity to Information Sharing Platforms	NONE	NONE	NONE	NONE
T4.4.2	Information Released into Information Sharing Communities	NONE	NONE	NONE	NONE
T4.5.1	Network Controls	A.10.6.1	AC-4, AC-17, AC-18, AC-20, CA-3, CP-8, PE-5, SC-7, SC-8, SC-9, SC-10, SC-19, SC-20, SC-21, SC-22, SC-23	10.6.1	IS.11
T4.5.2	Security of Network Services	A.10.6.2	SA-9, SC-8, SC-9	10.6.2	IS.11
T4.5.3	Segregation in Networks	A.11.4.5	AC-4, SA-8, SC-7	11.4.5	IS.10
T4.5.4	Security of Wireless Networks	A.11.4.5	AC-4, SA-8, SC-7	11.4.5	IS.10

Control Number	Control Name	ISO 27001 ISO 27002	NIST SP800 – 53r4	ADSIC v1.0	ADSIC v2.0
T5.1.1	Access Control Policy	A.11.1.1	AC-1, AC-5, AC-6, AC-17, AC-18, AC-19, CM-5, MP-1, SI-9	11.1.1	IA.4
T5.2.1	User Registration	A.11.2.1	AC-1, AC-2, AC-21, IA-5, PE-1, PE-2	11.2.1	IA.2
T5.2.2	Privilege Management	A.11.2.2	AC-1, AC-2, AC-6, AC-21, PE-1, PE-2, SI-9	11.2.2	IA.4
T5.2.3	User Security Credentials Management	A.11.2.3	IA-5	11.2.3	IA.2
T5.2.4	Review of User Access Rights	A.11.2.4	AC-2, PE-2	11.2.4	IA.4
T5.3.1	Use of Security Credentials	A.11.3.1	IA-2, IA-5	11.3.1	IA.3
T5.4.1	Policy on Use of Network Services	A.11.4.1	AC-1, AC-5, AC-6, AC-17, AC-18, AC-20	11.4.1	IA.4
T5.4.2	User Authentication for External Connections	A.11.4.2	AC-17, AC-18, AC-20, CA-3, IA-2, IA-8	11.4.2	IA.5
T5.4.3	Equipment Identification in Networks	A.11.4.3	AC-19, IA-3	11.4.3	OM.15
T5.4.4	Remote Diagnostic and Configuration Protection	A.11.4.4	AC-3, AC-6, AC-17, AC-18, PE-3, MA-3, MA-4	11.4.4	OM.12
T5.4.5	Network Connection Control	A.11.4.6	AC-3, AC-6, AC-17, AC-18, SC-7	11.4.6	IS.10
T5.4.6	Network Routing Control	A.11.4.7	AC-4, AC-17, AC-18	11.4.7	IS.11
T5.4.7	Wireless Access	A.10.6.1, A.10.8.1, A.11.4.1, A.11.4.2, A.11.4.6, A.11.7.1	AC-18	11.4.2	IA.5
T5.5.1	Secure Log-oOn Procedures	A.11.5.1	AC-7, AC-8, AC-9, AC-10, IA-2, IA-6, IA-8, SC10	11.5.1	IA.2
T5.5.2	User Identification and Authentication	A.11.5.2	IA-2, IA-4, IA-5, IA-8	11.5.2	IA.1
T5.5.3	User Credentials Management System	A.11.5.3	IA-2, IA-5	11.5.3	IA.3

Control Number	Control Name	ISO 27001 ISO 27002	NIST SP800 – 53r4	ADSIC v1.0	ADSIC v2.0
T5.5.4	Use of System Utilities	A.11.5.4	AC-3, AC-6	11.5.4	OM.13
T5.6.1	Information Access Restriction	A.11.6.1	AC-3, AC-6, AC-14, CM-5	11.6.1	IA.4
T5.6.2	Sensitive System Isolation	A.11.6.2	SP 800-39	11.6.1	IA.4
T5.6.3	Publicly Accessible Content	A.10.9.3	AC-22, SC-14	10.9.3	NONE
T5.7.1	Access Control for Mobile Devices	A.11.7.1	AC-1, AC-17, AC-18, AC-19, PL-4, PS-6	11.7.1	IS.12
T5.7.2	Teleworking	A.11.7.2	AC-1, AC-4, AC-17, AC-18, PE-17, PL-4, PS-6	11.7.2	IA.5
T6.1.1	Third Party Security Policy	NONE	PS-7	NONE	NONE
T6.2.1	Service Delivery	A.10.2.1	SA-9	10.2.1	TP.3
T6.2.2	Monitoring and Review of Third Party Services	A.10.2.2	SA-9	10.2.2	TP.3
T6.2.3	Managing Changes to Third Party Services	A.10.2.3	RA-3, SA-9	NONE	NONE
T6.3.1	Information Security Requirements for Cloud Environments	NONE	NONE	NONE	NONE
T6.3.2	Service Delivery Agreements with Cloud Providers	NONE	NONE	NONE	NONE
T7.1.1	Information Systems Acquisition, Development and Maintenance Policy	NONE	SA-1, MA-1, SI-1	NONE	NONE
T7.2.1	Security Requirements Analysis and Specification	A.12.1.1	SA-1, SA-3, SA-4	12.1.1	IS.1
T7.2.2	Developer-Provided Training	NONE	SA-16	NONE	NONE
T7.3.1	Input Data Validation	A.12.2.1	SI-9, SI-10	12.2.1	IS.2
T7.3.2	Control of Internal Processing	A.12.2.2	SI-7, SI-9, SI-10	12.2.2	IS.2
T7.3.3	Message Integrity	A.12.2.3	AU-10, SC-8, SI-7	12.2.3	IS.2
T7.3.4	Output Data Validation	A.12.2.4	No Mapping	12.2.4	IS.2

Control Number	Control Name	ISO 27001 ISO 27002	NIST SP800 – 53r4	ADSIC v1.0	ADSIC v2.0
T7.4.1	Policy on the Use of Cryptographic Controls	A.12.3.1	Multiple controls address cryptography (e.g., IA-7, SC-8, SC-9, SC-12, SC-13)	12.3.1	IS.5
T7.4.2	Key Management	A.12.3.2	SC-12, SC-17	12.3.1	IS.5
T7.5.1	Control of Operational Software	A.12.4.1	CM-1, CM-2, CM-3, CM-4, CM-5, CM-9, PL-4, SA-6, SA-7	12.4.1	OM.1
T7.5.2	Protection of System Test Data	A.12.4.2	Multiple controls; protection of test data not addressed separately in SP 800-53 (e.g., AC-3, AC-4)	12.4.2	IS.15
T7.5.3	Access Control to Program Source Code	A.12.4.3	AC-3, AC-6, CM-5, CM-9, MA-5, SA-10	12.4.3	IS.4
T7.6.1	Change Control Procedures	A.12.5.1	CM-1, CM-3, CM-9, SA-10	12.5.1	OM.2
T7.6.2	Technical Review of Applications After Operating System Changes	A.12.5.2	CM-3, CM-4, CM-9, SI-2	12.5.2	OM.2
T7.6.3	Restrictions on Changes to Software Packages	A.12.5.3	CM-3, CM-4, CM-5, CM-9	12.5.3	OM.2
T7.6.4	Information Leakage	A.12.5.4	AC-4, PE-19	12.5.4	IS.6
T7.6.5	Outsourced Software Development	A.12.5.5	SA-1, SA-4, SA-6, SA-7, SA-8, SA-9, SA-11, SA-12, SA-13	12.5.5	TP.2
T7.7.1	Control of Technical Vulnerabilities	A.12.6.1	RA-3, RA-5, SI-2, SI-5	3.4.1	OM.7
T7.8.1	Supply Chain Protection Strategy	NONE	SA-12	NONE	NONE
T7.8.2	Supplier Reviews	NONE	SA-12	NONE	TP.1
T7.8.3	Limitation of Harm	NONE	SA-12	NONE	NONE
T7.8.4	Supply Chain Operations Security	NONE	SA-12	NONE	NONE
T7.8.5	Reliable Delivery	NONE	SA-12	NONE	NONE
T7.8.6	Processes to Address Weaknesses or Deficiencies	NONE	SA-12	NONE	NONE

Control Number	Control Name	ISO 27001 ISO 27002	NIST SP800 – 53r4	ADSIC v1.0	ADSIC v2.0
T7.8.7	Supply of Critical Information System Components	NONE	SA-12	NONE	NONE
T8.1.1	Information Security Incident Management Policy	NONE	IR-1	NONE	NONE
T8.2.1	Incident Response Plan	A.13.2.1	IR-8	NONE	IM.4
T8.2.2	Computer Security Incident Response Team	NONE	Partially (IR-10)	NONE	IM.2
T8.2.3	Incident Classification	NONE	NONE	NONE	IM.4 (Partially)
T8.2.4	Incident Response Training	NONE	IR-2	NONE	NONE
T8.2.5	Incident Response Testing	NONE	IR-3	14.1.5	IM.8.3
T8.2.6	Incident Response Assistance	NONE	IR-7	NONE	IM.8.1, IM.8.5
T8.2.7	Information Security Incident Documentation	NONE	NONE	NONE	IM.7
T8.2.8	Learning From Information Security Incidents	A.13.2.2	IR-4	13.2.3	NONE
T8.2.9	Collection of Evidence	A.13.2.3	AU-9, IR-4	13.2.4	IM.5
T8.3.1	Situational Awareness	NONE	PM-16	NONE	IM.6.6
T8.3.2	Reporting Information Security Events	A.13.1.1	AU-6, IR-1, IR-6, SI-4, SI-5	13.1.1	IM.3
T8.3.3	Reporting Security Weaknesses	A.13.1.2	PL-4, SI-2, SI-4, SI-5	13.1.2	IM.3.4 (Partially)
T9.1.1	Information Systems Continuity Planning Policy	NONE	CP-1	14.1.1	IC.1
T9.2.1	Developing Information Systems Continuity Plans	A.14.1.3	CP Family	14.1.3	IC.3
T9.2.2	Implementing Information Systems Continuity Plans	A.14.1.3	CP Family	14.1.3	IC.3
T9.3.1	Testing, Maintaining and Re-Assessing Information Systems Continuity Plans	A.14.1.5	CP-2, CP-4, CP-5	14.1.5	IC.4

Annex D: Mapping of Threats to Controls

The following table provides examples of typical threats along with their mitigating controls. The list of threats types are aggregated from benchmark risk registers and mapped to mitigating controls to assist implementing entities during their risk assessment process.

Overall, a number of security controls are needed to mitigate specific threat types given the complex nature of the threats. As such, threat types along with their corresponding mitigating controls are outlined in Table 9 below.

Table 9: Mapping of Threats to Controls

Threat Type	Control Numbers of Mitigating Controls
Malware	
KeyLogger / Form-Grabber / Spyware	M3.3.3; M4.4.3; T1.4.1; T3.4.1; T3.4.2; T3.6.2; T3.6.3; T3.6.4; T4.5.1; T4.5.3; T5.2.1; T5.2.2; T5.2.3; T5.2.4; T5.3.1; T5.4.4; T5.4.5; T5.4.6; T5.5.1; T5.5.2; T5.5.3; T5.6.1; T7.7.1
Send Data to External Site/Entity	T1.4.1; T4.5.1; T5.4.2; T5.4.5; T5.5.1; T5.5.2; T5.5.3; T6.2.1; T6.2.2; T6.2.3; T6.3.1; T6.3.2
Backdoor or Command and Control	M4.4.3; T1.4.1; T1.4.2; T3.4.1; T3.4.2; T3.5.1; T3.6.2; T3.6.3; T3.6.4; T3.6.5; T4.5.1; T4.5.2; T4.5.3; T4.5.4; T5.2.1; T5.2.2; T5.2.3; T5.2.4; T5.3.1; T5.4.2; T5.4.3; T5.4.5; T5.4.7; T5.5.1; T5.5.2; T5.5.3; T5.6.1; T5.6.2; T7.7.1
Disable or interfere with security controls	T2.2.1; T2.2.2; T2.2.3; T2.2.5; T2.2.6; T2.3.8; T3.4.1; T3.4.2; T3.6.2; T5.2.3; T5.2.4; T5.3.1; T5.4.2; T7.3.3; T7.6.2; T7.6.3; T7.7.1
System / Network Utilities	T2.3.2; T3.4.1; T3.4.2; T4.5.1; T4.5.2; T4.5.4; T5.4.7; T5.5.4; T5.6.2
RAM Scraper	T2.3.9; T3.4.1; T3.4.2; T3.6.3; T3.6.4; T3.6.5; T4.3.1; T4.3.2; T4.5.2; T5.4.2; T5.5.1; T5.5.2; T7.4.1; T7.4.2; T7.6.4; T7.7.1
Data from Untrustworthy Sources	M3.3.3; M3.4.1; T3.4.1; T5.5.2
Capture Data Resident on System	T3.2.5; T3.4.1; T3.4.2; T3.6.4; T4.5.3
Download/Install additional Malware or Updates	T1.4.1; T3.4.1; T3.4.2; T3.5.1; T5.2.1; T5.2.2; T5.2.3; T5.2.4; T5.3.1; T7.5.3; T7.6.3; T7.6.5
Redirect to another site/address	T3.4.1; T3.4.2; T5.4.2

Threat Type	Control Numbers of Mitigating Controls
Hacking	
Exploitation of default or guessable credentials	M1.3.7; T4.5.3; T4.5.4; T5.2.4; T4.4.7; T5.5.1; T5.5.3; T6.1.1; T6.2.2
Use of Stolen Login Credentials	M4.4.3; T3.6.2; T3.6.3; T3.6.5; T4.5.1; T4.5.2; T4.5.3; T5.1.1; T5.2.1; T5.2.2; T5.2.3; T5.2.4; T5.3.1; T5.4.1; T5.4.3; T5.4.5; T5.5.1; T5.5.2; T5.5.3; T5.6.1
Brute Force and Dictionary Attacks	T5.1.1; T5.2.1; T5.2.2; T5.2.3; T5.2.4; T5.3.1; T5.4.2; T5.5.1; T5.5.3
Exploitation of backdoor or command and control channels	M4.4.3; T1.4.1; T1.4.2; T3.4.1; T3.4.2; T3.5.1; T3.6.2; T3.6.3; T3.6.4; T3.6.5; T4.5.1; T4.5.2; T4.5.3; T5.2.1; T5.2.2; T5.2.3; T5.2.4; T5.3.1; T5.4.2; T5.4.3; T5.4.5; T5.5.1; T5.5.2; T5.5.3; T5.6.1; T5.6.2; T7.7.1
Authentication Bypass	M5.4.1; T3.5.1; T3.6.3; T3.6.4; T3.6.5; T4.5.1; T4.5.3; T5.4.3; T5.4.5; T5.4.6; T5.5.3; T5.6.1; T7.7.1; T7.8.6
SQL Injection	M5.4.1; T1.4.1; T3.2.5; T3.4.1; T3.4.2; T3.5.1; T3.6.3; T3.6.4; T4.5.1; T5.2.2; T5.5.2; T6.3.1; T7.3.1; T7.3.2; T7.3.3; T7.3.4; T7.5.2; T7.7.1; T7.8.6
Denial of Service (DOS) or DDOS	T3.2.1; T4.5.2; T4.5.4; T5.4.7; T4.5.3
Remote File Inclusion	T3.2.1; T3.4.1; T3.4.2; T4.5.1; T4.5.2; T7.4.1; T7.4.2; T7.7.1
Abuse of Functionality	T5.2.2; T5.2.3; T5.2.4; T5.3.1; T5.4.4; T5.4.5; T5.5.1; T5.7.1; T7.3.4; T7.4.1; T7.4.2; T7.6.3; T7.8.3
Remote Spying	M4.4.2; M5.2.3; M5.2.4; T3.4.1; T3.4.2; T3.6.1; T3.6.3; T3.6.4; T3.6.5; T4.5.1; T4.5.3; T5.1.1; T5.2.1; T5.2.3; T5.3.1; T5.4.2; T5.4.3; T5.4.5; T5.5.1; T5.5.2; T5.6.1; T5.6.2; T7.4.1; T7.4.2; T7.7.1; T7.8.5
Eavesdropping / Packet Sniffing	T2.2.1; T2.2.2; T4.1.1; T4.2.1; T4.2.2; T4.2.3; T4.2.4; T4.3.1; T4.3.2; T4.5.1; T5.4.3; T5.4.6; T7.4.1
Social	
Pretexting	M3.4.1; M4.1.1; M4.3.1; M4.3.2; T5.1.1; T5.6.1; T5.6.3
Intentional Leaks / Sharing of Data by Staff	M3.4.1; M4.1.1; M4.2.1; M4.3.2; M5.2.3; M5.2.4; T3.6.3; T5.1.1; T5.2.2; T5.2.4; T5.4.2; T5.5.2; T5.6.1; T7.6.4
Phishing	M3.3.3; M3.4.1; M4.1.1; T3.4.1; T3.4.2; T4.1.1; T4.2.1; T5.1.1; T5.5.1; T5.5.2; T5.5.3
Accidental Leaks / Sharing of Data by Staff	M3.3.3; M3.4.1; M5.2.3; T3.6.3; T5.1.1; T5.2.2; T5.4.2; T5.5.2; T5.6.1; T5.6.3; T7.6.4
Illegal Processing of Data	M3.3.3; M3.4.2; M4.2.1; M4.3.2; M4.4.3; M5.2.2; M5.2.3; M5.2.7; T1.3.1; T1.3.2; T3.2.4; T3.5.1; T3.6.3; T4.2.1; T4.2.4; T5.2.2; T5.2.3; T5.2.4; T5.3.1; T5.4.2; T5.4.3; T5.5.2; T5.5.3; T5.6.1; T5.6.2

Threat Type	Control Numbers of Mitigating Controls
Misuse	
Embezzlement, Skimming, and Related Fraud	T1.2.2; T1.2.3; T1.3.2; T1.4.1; T1.4.2
Use of Unapproved Hardware/ Devices	M1.3.1; M1.3.6; M1.1.3; M5.2.5; T1.1.1; T1.2.1; T1.2.2; T1.2.3; T1.3.3; T2.3.4; T3.2.4; T3.3.2; T3.6.3; T5.4.3; T7.7.1
Abuse of System Access/Privileges	M4.4.1; M4.4.3; T3.2.4; T4.5.1; T4.5.3; T5.2.1; T5.2.2; T5.2.3; T5.2.4; T5.5.2; T7.6.4
Retrieval of Recycled or Discarded Media	M4.4.2; T1.1.1; T1.2.1; T1.4.1; T1.4.2; T2.3.6; T3.4.1; T3.4.2
Equipment Failure	T2.3.1; T2.3.4; T3.2.1; T3.2.4; T3.3.2; T3.5.1; T3.6.2; T3.6.3; T3.6.6; T3.6.7; T5.4.3; T7.3.1; T7.3.2; T7.3.4; T9.2.1; T9.2.2; T9.3.1
Equipment Malfunction	M3.3.2; M3.3.3; M5.2.5; T1.2.2; T1.3.3; T3.2.1; T3.2.2; T3.2.4; T3.3.2; T3.5.1; T3.6.2; T3.6.3; T3.6.6; T3.6.7; T5.4.3; T7.7.1; T9.2.1; T9.2.2; T9.3.1
Software Malfunction	M3.3.2; M3.3.3; T1.2.2; T3.2.1; T3.2.2; T3.2.4; T3.3.2; T3.5.1; T3.6.2; T3.6.3; T3.6.6; T7.2.2; T7.3.1; T7.3.2; T7.3.4; T7.5.1; T7.5.3; T7.6.2; T7.6.3; T7.6.5; T7.7.1; T9.2.1; T9.2.2; T9.3.1
Error in Use	M3.3.1; M3.3.2; M3.3.3; M3.4.1; M5.2.5; T3.2.2; T3.5.1; T3.6.3; T3.6.6
Use of Counterfeit or Copied Software	T1.2.2; T3.2.4; T3.2.5; T3.3.2; T7.3.1; T7.3.2; T7.3.4; T7.5.1; T7.6.3; T7.6.5
Misappropriation of Private Knowledge	M3.3.2; M3.3.3; M3.4.1; T1.3.1; T1.3.2; T1.4.1; T1.4.2; T2.2.1; T2.2.2; T2.2.3; T2.2.5; T2.2.6; T2.3.6; T2.3.8; T4.2.3; T4.3.1; T4.3.3; T4.4.1; T4.4.2; T5.2.2; T5.2.3; T5.2.4; T5.7.1; T5.7.2
Inappropriate Web/Internet Usage	M3.4.1; T3.4.1; T4.3.1; T4.3.2; T4.5.1; T4.5.2; T5.2.2; T5.4.2
Physical	
Tampering	M3.2.1; M3.3.1; M3.4.1; M5.4.1; T2.2.3; T2.3.1; T2.3.4; T2.3.5; T2.3.8; T3.4.1; T3.4.2; T3.5.1; T3.6.3; T3.6.5; T5.2.3; T5.4.2; T5.4.4; T5.5.2; T7.5.3; T7.6.2; T7.6.3; T7.7.1
Major Accident	T2.1.1; T2.2.3; T2.2.4; T2.3.1; T3.5.1; T8.1.1; T8.3.2; T8.2.1; T8.2.2; T8.3.1; T8.2.3; T8.2.4; T8.2.5; T8.2.7; T9.1.1; T9.2.1; T9.2.2; T9.3.1
Destruction of Equipment or Media	T1.1.1; T1.2.2; T1.2.3; T1.4.1; T2.1.1; T2.2.1; T2.2.2; T2.2.3; T2.3.1; T2.3.5; T2.3.8; T3.2.4; T3.5.1; T9.1.1; T9.2.1; T9.2.2; T9.3.1
Physical Theft of Asset - Including Document, Media and Equipment	M3.3.3; M3.4.1; M4.3.2; M4.4.2; T1.1.1; T1.2.1; T1.2.2; T1.4.1; T1.4.2; T2.2.1; T2.2.2; T2.2.3; T2.3.1; T2.3.7; T2.3.8; T2.3.9; T3.5.1; T5.6.2; T7.4.1; T7.4.2
Unauthorized Use of Equipment	M1.3.1; M4.4.1; M5.2.5; T1.2.2; T2.3.1; T2.3.5; T3.2.4; T3.6.3; T5.2.3; T5.3.1; T5.5.2
Corruption of Data	T3.5.1; T4.2.3; T4.2.4; T4.5.3; T7.3.2; T7.3.3; T7.3.4

Annex E: Sector and National Level Controls

The following table provides a list of the sector and national level security controls. As a recap, sector and national level controls are designed to overcome the silos created by a single-entity approach to IA, and hence create a stronger and more integrated approach for national information assurance. They serve as foundational elements for developing the sector and national views of IA by enabling the integration and analysis of information relating to security threats, risks and incidents, as well as the state of these implementation and risk assessment outcomes.

Overall, the UAE IA Regulation provides a total of 15 sector and national level controls as outlined in Table 10 below.

Table 10: Sector and National Level Controls

Control Number	Control Name
M6 - Performance Evaluation and Improvement	
M1.3 – Organization of Information Security	
M1.3.3	Contact with Authorities
M1.3.4	Contact with Special Interest Groups
M5 – Compliance	
M5.1 – Compliance Policy	
M5.1.1	Compliance Policy
T3 – Operations Management	
T3.6 – Monitoring	
T3.6.1	Monitoring Policy and Procedures
T4 – Communications	
T4.4 – Information Exchanges Protection	
T4.4.1	Connectivity to Information Sharing Platforms
T4.4.2	Information Released into Information Sharing Communities
T7 – Information Systems Acquisition, Development and Maintenance	
T7.4 – Cryptographic Controls	
T7.4.1	Policy on the Use of Cryptographic Controls

Control Number	Control Name
T7.8 – Supply Chain Management	
T7.8.1	Supply Chain Protection Strategy
T7.8.2	Supplier Reviews
T8 – Information Security Incident Management	
T8.1 – Information Security Incident Management Policy	
T8.1.1	Reporting Information Security Events
T8.3 – Information Security Events and Weaknesses Reporting	
T8.3.2	Information Security Incident Response Policy
T8.2 – Management of Information Security Incidents and Improvements	
T8.2.2	Incident Classification
T8.3 – Information Security Events and Weaknesses Reporting	
T8.3.1	Situational Awareness

Annex F: Terms and Definitions

Table 11: Terms and Definitions

Term	Definition
Asset	Anything that has value to the organization such as software, information, information systems.[4]
Audit	An independent review of event logs and related activities performed to determine the adequacy of current security measures, to identify the degree of conformance with established policy or to develop recommendations for improvements to the security measures currently applied
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See Authentication.
Availability	The property of being accessible and usable upon demand by an authorized entity [4]
Certification	A procedure by which a formal assurance statement is given that a deliverable conforms to a specified standard

Term	Definition
Cloud Computing	The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes[4]
Control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature[4] Note: Control is also used as a synonym for safeguard or countermeasure
Critical Entity	An entity responsible for the investments in, and/or day-to-day operation of a particular critical information infrastructure
Critical Information Infrastructure	Physical and virtual information assets that support carrying-out of a critical function and the delivery of a critical service.
Critical Information Infrastructure Operator	An entity responsible for the investments in, and/or day-to-day operation of, a particular critical information infrastructure
Critical Information Infrastructure Protection	The protection of critical information infrastructure such as information assets, that support the delivery of a critical service
Critical Sector	A sector identified at the national level that provides critical service(s).
Critical Service	Vital service, the disruption or destruction of which may have a debilitating impact on the national security, economy, society or any combination of these.
Cryptographic System	A related set of hardware or software used for cryptographic communication, processing or storage, and the administrative framework in which it operates
Cybersecurity	Cybersecurity is the set of technologies, processes, legislations, practices, and other required capabilities designed to protect the information infrastructure from disruption, breakdown, or misuse.
Cyberspace	Global electronic medium comprised of a network of interdependent information technology infrastructures, telecommunications networks and computer processing systems
Demilitarized Zone (or DMZ)	A small network with one or more servers that is kept separate from the core network, either on the outside of the firewall, or as a separate network protected by the firewall. Demilitarized zones usually provide public domain information to less trusted networks, such as the Internet
Entity Context	Refers to the set of entity information assets, practices, and standards that characterize core cyber security capabilities to establish a minimum level of information assurance within a given entity

Term	Definition
Filter	A hardware or software device that controls the flow of data in accordance with a security policy
Firewall	A network protection device that filters incoming and outgoing network data, based on a series of rules
Gateway	Gateways connect two or more networks from different security domains to allow access to or transfer of information according to defined security policies. Some gateways can be automated through a combination of physical or software mechanisms
Guideline	A description that clarifies what should be done and how, to achieve the objectives set out in policies [4]
Hacktivists	People that perform the act of hacking, or breaking into computer systems, for a politically or socially motivated purpose
Hardware	A generic term for any physical component of information and communication technology
Host-based Intrusion Detection System (HIDS or IDS) IATFs	A security device, resident on a specific host, which monitors system activities for malicious or unwanted behavior Information Assurance Technical Forums are governance bodies that engage key stakeholders (such as industry leaders, experts, relevant entities, and sector regulators) in the development of the UAE IA Regulation.
Implementing Entity	Refers to any entity implementing the UAE IA Regulation – including critical entities mandated to implement these , as well as any other entities implementing these .
Information Asset	A physical or virtual asset of ICT systems such as data, systems, facilities, network and computers.
Information Assurance	Practice of protecting information and managing risks related to the use, processing, storage and transmission of information or data, and the systems and processes used for those purposes.
Information Security	Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved [4].
Information Security Event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant[4].
Information Security Incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security[4]

Term	Definition
Information Security Policy	A high-level document that describes how an entity protects its systems. The ISP is normally developed to cover all systems and can exist as a single document or as a set of related documents
Information Sharing Capability	A set of policies, systems, and organizational roles needed to share information based on established requirements
Information sharing Community	Group of organizations that agree to share information
Integrity	The property of safeguarding the accuracy and completeness of assets[4]
Key Management	The use and management of cryptographic keys and associated hardware and software. It includes their generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction
Malicious Code or Malware	Any software that attempts to subvert the confidentiality, integrity or availability of a system. Types of malicious code include logic bombs, trapdoors, Trojans, viruses and worms
Management Controls Media	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information systems security A generic term for hardware that is used to store information
Media Disposal	The process of relinquishing control of media when no longer required, in a manner that ensures that no data can be recovered from the media
National Context	Refers to the set of national information assets, practices, and standards that characterize core cyber security capabilities to establish a minimum level of information assurance at a national level
National Cyber Response Framework	The program designed to increase situational awareness, rapidly identify and analyze incidents, and coordinate responses with national cyber security stakeholders
Network Device	Any device designed to facilitate the communication of information destined for multiple system users. For example: cryptographic devices, firewalls, routers, switches and hubs
Non-Repudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.
Policy	Overall intention and direction as formally expressed by management[4]
Regulator	A government body that sets and monitors compliance and behavior of regulated entities in a particular sector (or market)

Term	Definition
Remote Access	Access to a system from a location not under the physical control of the system owner
Removable Media	Storage media that can be easily removed from a system and is designed for removal
Residual risk	The risk remaining after risk treatment[4]
Risk	Combination of the probability of an event and its consequence[4]
Risk acceptance	Decision to accept a risk[4]
Risk analysis	Systematic use of information to identify sources and to estimate the risk[4] Overall process of risk analysis and risk evaluation[4]
Risk assessment Risk evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk[4]
Risk management	Coordinated activities to direct and control an organization with regard to risk[4]
Risk treatment	Process of selection and implementation of measures to modify risk[4] NOTE: In this International Standard the term 'control' is used as a synonym for 'measure'
Sector Plan	Detailed plan developed by sector regulator and approved by NCSA outlining the actions, responsible entities and timelines necessary to address the highest levels of risk identified in the Sector/National Risk Assessments and guide implementation of related CII Cybersecurity and Protection Requirements.
Sector-Specific CIIP Working Group	Sector-specific governance body, chaired by NCSA and comprised of sector regulator, operators and other stakeholders to foster sector collaboration and support sector planning, implementation, and monitoring activities to elevate Critical Information Infrastructure Protection
Software Component	An element of a system, including but not limited to, a database, operating system, network or web application
Statement of applicability	Documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS. NOTE: Control objectives and controls are based on the results and conclusions of the risk assessment and risk treatment processes, legal or regulatory requirements, contractual obligations and the organization's business requirements for information security
Supply Chain	The sequence of processes involved in the production and distribution of a product or a service

Term	Definition
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system
Third party	That person or body that is recognized as being independent of the parties involved, as concerns the issue in question[4]
Threat	A potential cause of an unwanted incident, which may result in harm to a system or organization[4]
Threat Agent	Any person or thing that acts - or has the power to act - to cause, carry, transmit, or support a threat
Threat Vector	The method a threat uses to get to the target
Trusted information communication entity	Autonomous organization supporting information exchange within an information sharing community
Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more threats[4]
Wireless Communications	The transmission of data over a communications path using electromagnetic waves rather than a wired medium

[4] The definition is based on ISO/IEC Publications.

Annex G: Bibliography

Table 12: Bibliography

#	Reports and Standards
1	**ISO/IEC 27001:2005** "Information technology — Security techniques — Information security management systems — Requirements"
2	**ISO/IEC 27002:2005** "Information technology — Security techniques — Code of practice for Information security management"
3	**ISO/IEC 27005:2005** "Information technology — Security techniques —Information security risk management"
4	**ISO/IEC 27010:2012** "Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications"
5	**ISO/IEC 27032:2012** "Information technology — Security techniques — Guidelines for cybersecurity"
6	SANS 20 Critical Security Controls for Effective Cyber Defense, Version 4.1
7	**NIST 800-53 Revision 4** "Security and Privacy Controls for Federal Information Systems and Organizations"
8	Abu Dhabi Information Security Standards, Version 1 and Version 2
9	Verizon Data Breach Investigation Report, 2012
10	Symantec Internet Security Threat Report, April 2012
11	Kaspersky Global IT Security Risks, 2012
12	Microsoft Security Intelligence Report, June 2012