GOVERNMENT OF BANGLADESH INFORMATION SECURITY MANUAL

BANGLADESH COMPUTER COUNCIL
MINISTRY OF INFORMATION & COMMUNICATION TECHNOLOGY

1. Document information

Project Name	Development of Information Security Policies, standards, and National Computer Incident Response Team (CIRT) implementation (International) - BGD e-GOV CIRT
Client Representatives	Tarique M Barkatullah Md. Tawhidur Rahman, C|CISO
Contract Package	S11
Credit	5025-BD
Document Date	18 February 2016
Version Date	29 February 2016
Version	1.5
Document Number	BCC-CIRT-0036
Document Type	Formal
Document Status	Final
Prepared by	Md. Sabbir Hossain, C|CISO
Reviewed by	Sigitas Rokas, CISM
Review Date	29 February 2016
Additional information	This document is based on International Standards ISO/IEC 27001:2013, ISO/IEC 27002:2013, and New Zealand Information Security Manual (NZISM)

Table of Contents

1. Document information 1
2. Executive summary 6
3. What is an information security manual and what does it define? 7
4. Applicability, Authority and Compliance 9
5. Information Security within Government 10
   5.1. Government Engagement 10
   5.2. Industry Engagement and Outsourcing 10
6. Information Security Governance – Roles and Responsibilities 12
   6.1. The Agency Head 12
   6.2. The Chief Information Security Officer 12
   6.3. Information Technology Security Managers 15
   6.4. System Owners 17
   6.5. System Users 18
7. System Certification and Accreditation 20
   7.1. The Certification and Accreditation Process 20
   7.2. Conducting Certifications 23
   7.3. Conducting Audits 23
   7.4. Accreditation Framework 25
   7.5. Conducting Accreditations 26
8. Information Security Documentation 28
   8.1. Documentation Fundamentals 28
   8.2. Information Security Policies (SecPol) 29
   8.3. Security Risk Management Plans (SRMP) 30
   8.4. System Security Plans (SecPlan) 31
   8.5. Standard Operating Procedures (SOP) 32
   8.6. Incident Response Plans (IRP) 35
9. Information Security Monitoring 37
   9.1. Information Security Reviews 37

9.2. Vulnerability Analysis 38
9.3. Change Management 39
9.4. Business Continuity and Disaster Recovery 40
10. Information Security Incidents 42
10.1. Detecting Information Security Incidents 42
10.2. Reporting Information Security Incidents 43
10.3. Managing Information Security Incidents 44
11. Physical Security 47
11.1. Facilities 47
11.2. Servers and Network Devices 47
11.3. Network Infrastructure 48
11.4. IT Equipment 49
11.5. Tamper Evident Seals 49
12. Personnel Security 51
12.1. Information Security Awareness and Training 51
12.2. Authorizations and Briefings 53
12.3. Using the Internet 54
13. Infrastructure 56
13.1. Cable Management Fundamentals 56
13.2. Cable Management for Non-Shared Government Facilities 56
13.3. Cable Management for Shared Government Facilities 56
13.4. Cable Management for Shared Non-Government Facilities 57
13.5. Cable Labelling and Registration 58
14. Communication Systems and Devices 60
14.1. Fax Machines, Multifunction Devices and Network Printers 60
15. Product Security 62
15.1. Product Selection and Acquisition 62
15.2. Product Patching and Updating 63
15.3. Product Sanitization and Disposals 65

16. Decommissioning and Disposal 66
16.1. System Decommissioning 66
16.2. Media Usage 68
16.3. Media Sanitization 69
16.4. Media Destruction 70
17. Software Security 71
17.1. Standard Operating Environments 71
17.2. Application Whitelisting 74
17.3. Web Applications 75
17.4. Software Application Development 77
17.5. Web Application Development 78
18. Email Security 80
18.1. Email Applications 80
18.2. Email Infrastructure 80
19. Access Control 84
19.1. Identification and Authentication 84
19.2. System Access 87
19.3. Privileged Access 87
19.4. Remote Access 88
19.5. Event Logging and Auditing 88
20. Cryptography 91
20.1. Cryptographic Fundamentals 91
20.2. Secure Sockets Layer and Transport Layer Security 91
20.3. Secure Shell 92
20.4. Secure Multipurpose Internet Mail Extension 94
20.5. Open PGP Message Format 94
20.6. Internet Protocol Security 95
20.7. Key Management 96
21. Network Security 99

21.1. Network Management 99
21.2. Wireless Local Area Networks 101
21.3. Video and Telephony Conferencing and Internet Protocol Telephony 105
21.4. Intrusion Detection and Prevention 107
21.5. Gateways 109
21.6. Firewalls 111
21.7. Diodes 112
21.8. Session Border Controller 112
22. Working Off-Site 116
22.1. Agency Owned Mobile Devices 116
22.2. Working outside the Office 117
22.3. Non-Agency Owned Devices and Bring Your Own Device (BYOD) 117
23. Enterprise System Security 123
23.1. Cloud Computing 123
23.2. Virtualization 125
24. Annexure 128
24.1. Annex 1- Impact Classification System 128
24.2. Annex 2 -Threat Vector Analysis 129
24.3. Annex 3 - Cause Analysis 130
24.4. Annex 4 - Incident response plan, policy & Procedure Creation 131
24.5. Annex 6 – Access Control Event Logging 131
25. References 133

2. Executive summary

This report on the development of Information Security Manual for the Government of Bangladesh information (GOBISM) provides a final version of GOBISM.

This document is based on International Standards ISO/IEC 27001:2013 and ISO/IEC 27002:2013, which we consider to be best international standards governing information security in organizations and we expect to see the increasing number of organizations implementing those standards in the near future. Besides, the GOBISM follows the framework and controls established in New Zealand Information Security Manual (NZISM)(report on this matter was provided to Bangladesh Computer Council along with the reports on Australian ISM[1], UK ISM[2] and US ISM[3]on 9th of February, 2016).

We believe that by following best international practices in information security management, merging two outstanding documents (ISO/IEC 270xx standards and New Zealand Information Security Manual) and adapting them for the needs of the Government of Bangladesh we are able to provide the Bangladesh Computer Council with:

- solid, flexible and implementable information security manual that covers every important aspect of information security that needs to be implemented by government agencies in order to ensure the protection of their systems and information
- a set of information security principles and measures that could be translated into Government legal acts, policies and standards pertaining to Bangladesh information security
- a solid framework and set of controls for accreditation and certification of government systems
- a flexible way for risk management based on government agencies needs and priorities
- a smooth option to expand the GOBISM and make it applicable to classified information, if required

[1]Australian ISM (ASD)
2 UKISM (GCHQ)
3 USISM (NIST)

3. What is an information security manual and what does it define?

The Government of Bangladesh Information Security Manual (GOBISM) details processes and controls that are important for the protection of Bangladesh Government unclassified information and systems.

This manual is intended for use by Bangladesh Government departments, agencies and organizations. Private sector organizations are also encouraged to use this manual.

This GOBISM governs information security principles and controls applicable to unclassified information. Classified government information shall have an additional set of principles and controls developed and approved at appropriate level.

The controls presented in GOBISM shall be applicable to all government unclassified systems and information.

The controls presented in GOBISM are divided into two categories:

- **Mandatory controls**: the use, or-non-use thereof is essential in order to effectively manage identified risk, unless the control is demonstrably not relevant to the respective system. The rational for non-use of mandatory controls must be clearly demonstrated to the Accreditation Authority as part of the certification process, before approval for exception is granted.
- **Recommended controls**: the use, or non-use thereof is considered good and recommended practice, but valid reasons for not implementing a control could exist. The residual risk of non-using recommended controls needs to be agreed and acknowledged by the Accreditation authority with formal auditable record of this consideration and decision.

System owners seeking a dispensation for non-compliance with any mandatory controls in this manual must be granted a dispensation by their Accreditation Authority.

System owners seeking a dispensation for non-compliance with mandatory controls must complete an agency risk assessment which documents:

- the reason(s) for not being able to comply with this manual
- the alternative mitigation measure(s) to be implemented
- the strength and applicability of the alternative mitigations
- an assessment of the residual security risk(s)
- a date by which to review the decision.

Agencies should review decisions to be non-compliant with any controls at least annually.

Agencies must retain a copy and maintain a record of the supporting risk assessment and decisions to be non-compliant with any mandatory controls from this manual. Where recommended controls

are not implemented, agencies must record and formally recognize that non-use of any controls without due consideration may increase residual risk for the agency. This residual risk must be agreed and acknowledged by the Accreditation Authority.

4. Applicability, Authority and Compliance

Agencies understand and follow the requirements of GOBISM. Protection of government information and systems is a core accountability

Protection of government information and systems is a core accountability of each governmental agency. The role of Information Security Manual is to promote a consistent approach to information assurance and information security across entire Government of Bangladesh.

GOBISM is intended to structure and assist the implementation of Bangladeshi laws and government policy on information security. Compliance with the GOBISM is not required as a matter of law. However, the controls in the GOBISM could be made binding on departments and agencies, either by legislation, or by Government direction.

Smaller government agencies may not always have sufficient staffing or budgets to comply with all the requirements of this manual. In such circumstances smaller agencies may choose to either operate on systems fully hosted by another agency using their information security policies and information security resources.

5. Information Security within Government

5.1. Government Engagement

Objective:	Security personnel are aware of and use information security services offered within the Bangladesh Government
Recommended Control 1:	IT and security personnel should familiarize themselves with the information security roles and services provided by Bangladesh Government organizations

There is a number of organizations that are involved in providing information security advice to government agencies. GOBISM provides contact information of the responsible agency, where other agencies can seek advice and assistance relating to the implementation on GOBISM and other issues related to information security.

The table below contains a brief description of the other organizations which have a role in relating to information security within government.

Organization	Services
Bangladesh Police	Law enforcement in relation to electronic crime and other high tech crime
Comptroller and Auditor General	Independent assurance over the performance and accountability of public sector organizations, including IT audit and better practice guides for areas including information security
Bangladesh Computer Council	Services to government agencies and critical infrastructure providers to assist them to defend against cyber threats
Ministry of Home Affairs	Guidance on risk management, authentication standards and e-gov services
Ministry of Commerce	Development, co-ordination and oversight of Bangladesh Government policy on e-commerce, online services and internet
National Archives	Provides information on the archival of Government information
Ministry of Law	Advice on how to comply with Privacy Act and related legislation

5.2. Industry Engagement and Outsourcing

Objective:	Industry handling government information implements the same security measures as government agencies
Recommended Control 1:	Where an agency has outsourced information technology services and functions, any ITSMs within the agency should be independent

	of the company providing the information technology services and functions.
Recommended Control 2:	Where an agency has outsourced information technology services and functions, they should ensure that the outsourced organization provides a single point of contact within the organization for all information assurance and security matters

Outsourcing is contracting an outside entity to provide essential business functions and processes that could be undertaken by the Agency itself.

If an agency engages an organization for the provision of information technology services and functions, and where that organization also provides the services of an Information Technology Security Manager, they need to ensure that there is no actual or perceived conflict of interest (See also Section 6.3 - Information Technology Security Managers).

When an agency engages a company for the provision of information technology services and functions, having a central point of contact for information security matters within the company will greatly assist with incident response and reporting procedures.

6. Information Security Governance – Roles and Responsibilities

6.1. The Agency Head

Objective:	The Agency Head endorses and is accountable for information security within their agencies
Mandatory Control 1:	Where the agency head devolves their authority, the delegate must be at least a member of the Senior Executive Team or an equivalent management position
Mandatory Control 2:	The agency head must provide support for the development, implementation and ongoing maintenance of information security processes within their agency
Recommended Control 1:	When the agency head devolves their authority the delegate should be the CISO
Recommended Control 2:	Where the head of a smaller agencies is not be able to satisfy all segregation of duty requirements because of scalability and small personnel numbers, all potential conflicts of interest should be clearly identified, declared and actively managed.

The Agency Head is an Accreditation Authority for that agency – see also 7.4Accreditation Framework.

When an agency head chooses to delegate their authority as the Agency's Accreditation Authority they should do so with careful consideration of all the associate risks, as they remain responsible for the decisions made by their delegate.

The CISO is the most appropriate choice for delegated authority as they should be a senior executive and hold specialized knowledge in information security and security risk management.

Without the full support of the agency head, IT and security personnel are less likely to have access to sufficient resources and authority to successfully implement information security within their agency. If an incident, breach or disclosure of information occurs in preventable circumstances, the relevant agency head will ultimately be held accountable.

6.2. The Chief Information Security Officer

Objective:	The Chief Information Security Officer (CISO) sets the strategic direction for information security within their agency

Objective:	The Chief Information Security Officer (CISO) sets the strategic direction for information security within their agency
Recommended Control 1:	Agencies should appoint a person to the role of CISO or have the role undertaken by an existing person within the agency
Recommended Control 2:	The CISO role should be undertaken by a member of the Senior Executive Team or an equivalent management position
Recommended Control 3:	Where the role of the CISO is outsourced, potential conflicts of interest in availability, response times or working with vendors should be identified and carefully managed
Recommended Control 4:	CISO should report directly to the agency head on matters of information security within the agency
Recommended Control 5:	CISO should develop and maintain a comprehensive strategic level information security and security risk management program within the agency aimed at protecting the agency's information
Recommended Control 6:	CISO should be responsible for the development of an information security communications plan
Recommended Control 7:	CISO should create and facilitate the agency security risk management process
Recommended Control 8:	CISO should be responsible for ensuring compliance with the information security policies and standards within the agency
Recommended Control 9:	CISO should be responsible for ensuring agency compliance with the GOBISM through facilitating a continuous program of certification and accreditation based on security risk management
Recommended Control 10:	CISO should be responsible for the implementation of information security measurement metrics and key performance indicators within the agency
Recommended Control 11:	CISO should provide strategic level guidance for agency ICT projects and operations
Recommended Control 12:	CISO should coordinate the use of external information security resources to the agency including contracting and managing the resources
Recommended Control 13:	CISO should be responsible for controlling the information security

Objective:	The Chief Information Security Officer (CISO) sets the strategic direction for information security within their agency
	budget
Recommended Control 14:	CISO should be fully aware of all information security incidents within the agency
Recommended Control 15:	CISO should coordinate the development of disaster recovery policies and standards within the agency to ensure that business-critical services are supported appropriately and that information security is maintained in the event of a disaster
Recommended Control 16:	CISO should be responsible for overseeing the development and operation of information security awareness and training programs within the agency

The requirement to appoint a member of the Senior Executive Team or an equivalent management position to the role of CISO does not require a new dedicated position be created in each agency.

Where multiple roles are held by the CISO (manager of business unit), potential conflicts of interest should be clearly identified and a mechanism implemented to allow independent decision making in areas where conflict may occur. Particular attention shall be paid to operational imperatives and security requirements conflict.

The CISO within an agency is responsible for facilitating communications between security personnel, ICT personnel and business personnel to ensure alignment of business and security objectives within the agency. The CISO is also responsible for providing strategic level guidance for the agency security program and ensuring compliance with national policy, standards, regulations and legislation.

Having the CISO coordinate the use of external information security resources will ensure that a consistent approach is being applied across the agency.

As the CISO is responsible for the overall management of information security within an agency, it is important that they report directly to the agency head on any information security issues.

To ensure that the CISO is able to accurately report to the agency head on information security issues within their agency it is important that they remain fully aware of all information security incidents within their agency.

6.3. Information Technology Security Managers

Objective:	Information Technology Security Managers (ITSM) provide information security leadership and management within their agency
Mandatory Control 1:	Agencies must appoint at least one ITSM within their agency
Mandatory Control 2:	ITSMs must be responsible for assisting system owners to obtain and maintain the accreditation of their systems
Mandatory Control 3:	ITSMs must be responsible for ensuring the development, maintenance, updating and implementation of Security Risk Management Plans (SRMPs), Systems Security Plans (SecPlan) and any Standard Operating Procedures (SOPs) for all agency systems
Recommended Control 1:	Where an agency is spread across a number of geographical sites, it is recommended that the agency should appoint a local ITSM at each major site
Recommended Control 2:	ITSMs should not have additional responsibilities beyond those needed to fulfill the role as outlined within this manual
Recommended Control 3:	ITSMs should work with the CISO to develop an information security program within the agency
Recommended Control 4:	ITSMs should undertake and manage projects to address identified security risks
Recommended Control 5:	ITSMs should identify systems that require security measures and assist in the selection of appropriate information security measures for such systems
Recommended Control 6:	ITSMs should consult with ICT project personnel to ensure that information security is included in the evaluation, selection, installation, configuration and operation of IT equipment and software
Recommended Control 6:	ITSMs should work with system owners, systems certifiers and systems accrediators to determine appropriate information security policies for their systems and ensure consistency with relevant GOBISM components
Recommended Control 7:	ITSMs should notify the Accreditation Authority of any significant change that may affect the accreditation of that system
Recommended Control 8:	ITSMs should liaise with vendors and agency purchasing and legal areas to establish mutually acceptable information security contracts and service-level agreements
Recommended Control 9:	ITSMs should conduct security risk assessments on the implementation of new or updated IT equipment or software in the existing environment and develop treatment strategies, if necessary
Recommended Control 10:	ITSMs should select and coordinate the implementation of controls

Objective:	Information Technology Security Managers (ITSM) provide information security leadership and management within their agency
	to support and enforce information security policies
Recommended Control 11:	ITSMs should provide leadership and direction for the integration of information security strategies and architecture with agency business and ICT strategies and architecture
Recommended Control 12:	ITSMs should provide technical and managerial expertise for the administration of information security management tools
Recommended Control 13:	ITSMs should work with the CISO to develop information security budget projections and resource allocations based on short-term and long-term goals and objectives
Recommended Control 14:	ITSMs should coordinate, measure and report on technical aspects of information security management to CISO
Recommended Control 15:	ITSMs should monitor and report to CISO on compliance with information security policies, as well as the enforcement of information security policies within the agency
Recommended Control 16:	ITSMs should provide regular reports on information security incidents and other areas of particular concern to the CISO
Recommended Control 17:	ITSMs should assess and report to CISO on threats, vulnerabilities, and residual security risks and recommend remedial actions
Recommended Control 18:	ITSMs should assist system owners and security personnel in understanding and responding to audit failures reported by auditors
Recommended Control 19:	ITSMs should assist and guide the disaster recovery planning team in the selection of recovery strategies and the development, testing and maintenance of disaster recovery plans
Recommended Control 20:	ITSMs should provide or arrange for the provision of information security awareness and training for all agency personnel
Recommended Control 21:	ITSMs should provide expert guidance on security matters for ICT projects
Recommended Control 22:	ITSM should keep the CISO and system owners informed with up-to-date information on current threats

ITSMs are executives within an agency that act as a conduit between the strategic directions provided by the CISO and the technical efforts of systems administrators. The main area of responsibility of an ITSM is that of the administrative and process controls relating to information security within the agency.

When agencies outsource their ICT services, ITSMs should be independent of any company providing ICT services. This will prevent any conflict of interest for an ITSM in conducting their duties.

As ITSMs have knowledge of all aspects of information security they are best placed to work with ICT projects within the agency to identify and incorporate appropriate information security measures.

As ITSMs are responsible for the operational management of information security projects and functions within their agency, they will be aware of their funding requirements and can assist the CISO to develop information security budget projections and resource allocations.

The CISO will coordinate the use of external information security resources to the agency, whilst ITSMs will be responsible for establishing contracts and service-level agreements on behalf of the CISO.

The CISO will set the strategic direction for information security within the agency, whereas ITSMs are responsible for managing the implementation of information security measures within the agency.

The CISO will oversee the development and operation of information security awareness and training programs within the agency. ITSMs will arrange delivery of that training to personnel within the agency.

To ensure the CISO remains aware of all information security issues within their agency and can brief their agency head when necessary, ITSMs will need to provide regular reports on policy developments, proposed system changes and enhancements, information security incidents and other areas of particular concern to the CISO.

Whilst the CISO will coordinate the development of disaster recovery policies and standards within the agency, ITSMs will need to guide the selection of appropriate strategies to achieve the direction set by the CISO.

6.4. System Owners

Objective:	**System owners obtain and maintain accreditation of their systems**
Mandatory Control 1:	Each system must have a system owner who is responsible for the operation and maintenance of the system
Mandatory Control 2:	System owners must obtain and maintain accreditation of their system(s)
Mandatory Control 3:	System owners must ensure the development, maintenance and implementation of complete, accurate and up to date SRMPs,

Objective:	System owners obtain and maintain accreditation of their systems
	SecPlans and SOPs for systems under their ownership. Such actions must be documented. See Section 19.5- Event Logging and Auditing
Mandatory Control 4:	System Owners involve the ITSM in the redevelopment and updates of the SRMPs, SecPlans, and SOPs
Recommended Control 1:	System owners should be a member of the Senior Executive Team or an equivalent management position, for large or critical agency systems

It is the responsibility of the management (or system owner) to prepare and validate assertions[4] relating to the governance, assurance and security of information systems, in accordance with national policy and related standards.

The system owner is responsible for the overall operation of the system and they may delegate the day-to-day management and operation of the system to a system manager or managers. System owners need to ensure that systems are accredited to meet the agency's operational requirements. If modifications are undertaken to a system the system owner will need to ensure that the changes are undertaken in an appropriate manner, documented adequately and that any necessary reaccreditation activities are completed.

All systems should have a system owner in order to ensure IT governance processes are followed and that business requirements are met.

It is strongly recommended that a system owner be a member of the Senior Executive Team or in an equivalent management position, however, this does not imply that the system manager(s) should also be at such a level.

6.5. System Users

Objective:	System users comply with information security policies and procedures within their agency
Mandatory Control 1:	All system users must comply with the relevant security policies and procedures for the systems they use
Mandatory Control 2:	All system users must protect account authenticators, must not share authenticators for accounts without approval and be

[4]Assertions are formal statements by management or system owners, which claim the completeness, accuracy and validity of evenets, presentations, disclosure, transactions and related assurance, risk and governance aspects of certification and accreditation.

Objective:	System users comply with information security policies and procedures within their agency
	responsible for all actions under their accounts
Mandatory Control 3:	All system users mustuse their access to only perform authorised tasks and functions
Mandatory Control 4:	System users that need to bypass security policies, procedures or mechanisms for any reason must seek formal authorisation from the CISO or the ITSM, if this authority has been specifically delegated to the ITSM

If agencies fail to develop and maintain a security culture where system users are complying with relevant security policies and procedures for the systems they are using, there is an increased security risk of a system user unwittingly assisting with an attack against a system.

7. System Certification and Accreditation

7.1. The Certification and Accreditation Process

Objective:	Executives and Security Practitioners understand the Certification and Accreditation (C&A) process and its role in information security governance and assurance

Certification and Accreditation is a fundamental governance and assurance process, designed to provide the Board, Chief Executive and senior executives confidence that information and its associated technology are well-managed, that risks are properly identified and mitigated and that governance responsibilities can demonstrably be met. It is essential for credible and effective information assurance governance.

C&A has two important stages where certification must be completed (} G accreditation can take place. It is based on an assessment of risk, the application of controls described in the GOBISM and determination of any residual risk.

Certification and Accreditation are separate and distinct elements, demonstrate segregation of duties and assist in managing any potential conflicts of interest. These are important attributes in good governance systems.

The acceptance of residual risk lies with the Chief Executive of each agency, or lead agency where sector or multi-agency systems are implemented.

The complete C&A process has several elements and stages, illustrated in the Block Diagram at the end of this section.

There are four groups of participant in C&A process:

- **System Owners**, responsible for the design, development, system documentation and system maintenance, including any requests for recertification or reaccreditation
- The **Certification Authority**, responsible for the review of information and documentation provided by the system owner to ensure the ICT system complies with minimum standards and the agreed design
- The **Assessor** or Auditor, who will conduct inspections, audits and review as instructed by the Certification Authority
- The **Accreditation Authority** who will consider the recommendation of the Certification Authority, determine the acceptable level of residual risk and issue the system accreditation, the authority to operate a system.

Certification is the assertion that an ICT system complies with the minimum standards and controls described in the GOBISM, any relevant legislation and regulation and other relevant standards. It is based on a comprehensive evaluation or systems audit. This process is described in Section 7.2 - Conducting Certifications.

Certification is evidence that due consideration has been paid to risk, security, functionality, business requirements and is a fundamental part of information systems governance and assurance.

The Certification Authority for all agency information systems is the CISO unless otherwise delegated by the Agency Head.

Accreditation is the formal authority to operate a system, evidence that governance requirements have been addressed and that the Chief Executive has fulfilled the requirement to manage risk on behalf of the organization and stakeholders. This element of the C&A process is described in Section 7.4 - Accreditation Framework.

Accreditation ensures that either sufficient security measures have been put in place to protect information that is processed, stored or communicated by the system or that deficiencies in such measures have been identified, assessed and acknowledged, including the acceptance of any residual risk.

The Accreditation Authority for agencies is the agency head or their delegate (senior executive or CISO).

Penetration tests are an effective method of identifying vulnerabilities that in a system or network testing existing security measures and testing the implementation of controls. Penetration testing is also very useful in validating the effectiveness of the defensive mechanisms. This testing provides an increased level of assurance when system certification and accreditation is undertaken. It also demonstrates prudent risk management.

A penetration test usually involves the use of intrusive methods or attacks conducted by trusted individuals, methods similar to those used by intruders or hackers. Care must be taken not to adversely affect normal operations while these tests are conducted.

Penetration tests can range from simple scans of IP addresses in order to identify devices or systems offering services with known vulnerabilities, to exploiting known vulnerabilities that exist in an unpatched operating system, applications or other software. The results of these tests or attacks are recorded, analyzed, documented and presented to the owner of the system. Any deficiencies should then be addressed.

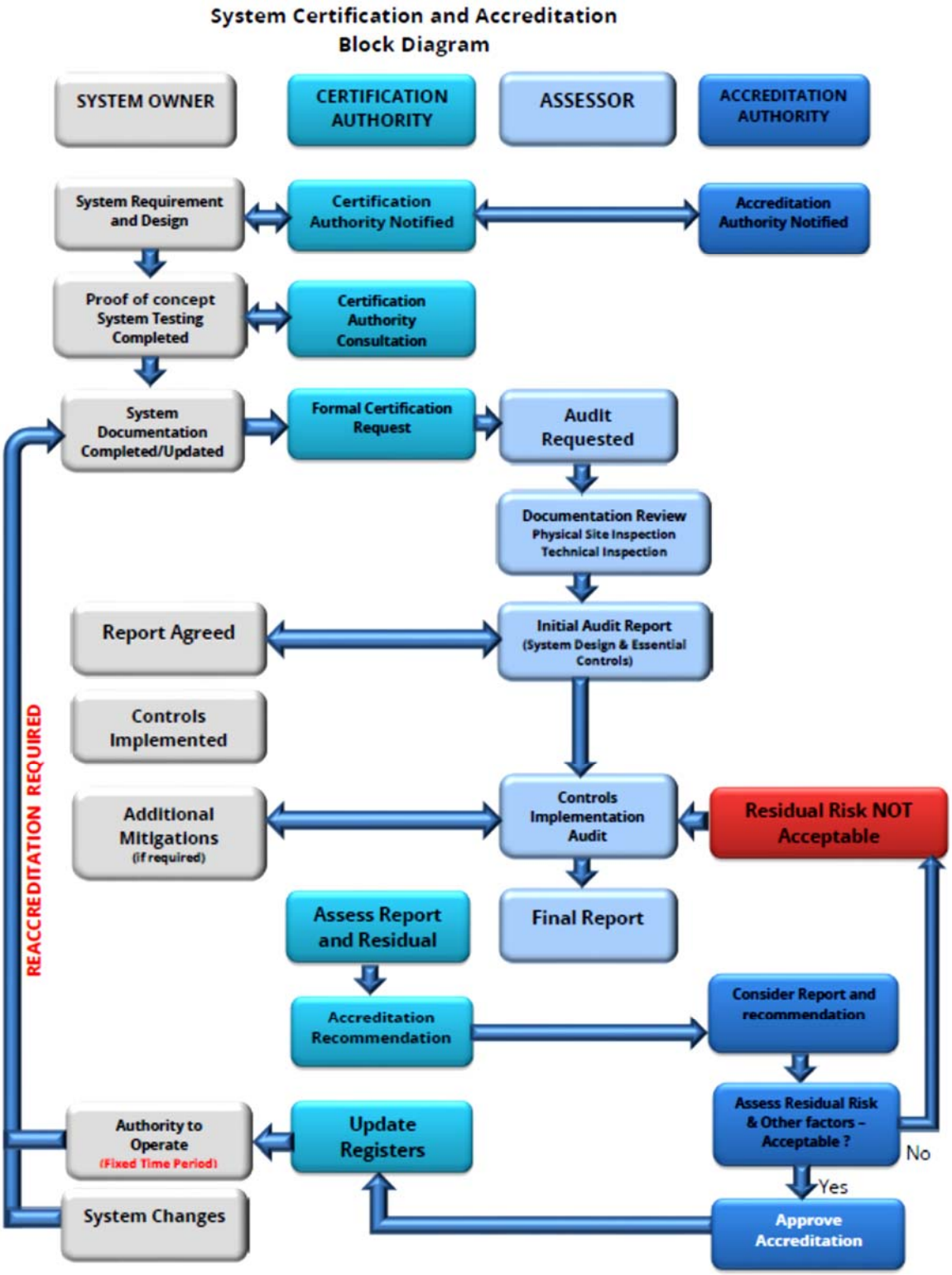

Figure 01: System Certification and Accreditation Block Diagram[5]

[5] Source: (NZISM, 2015)

7.2. Conducting Certifications

Objective:	**The security posture of the organization has been incorporated into its system security design, controls are correctly implemented, are performing as intended and that changes and modifications are reviewed for any security impact or implications**
Mandatory Control 1:	All systems must undergo an audit as part of the certification process
Mandatory Control 2:	The certification authority must accept that the controls are appropriate, effective and comply with the relevant GOBISM components, in order to award certification
Recommended Control 1:	Following the audit, the certification authority should produce an assessment for the Accreditation Authority outlining the residual security risks relating to the operation of the system and a recommendation on whether to award accreditation or not

The purpose of a Certification Audit is to assess the actual implementation and effectiveness of controls for a system against the agency's risk profile, security posture, design specifications, agency policies and compliance with the GOBISM components.

To award certification for a system the certification authority will need to be satisfied that the selected controls are appropriate and consistent with the relevant GOBISM components, have been properly implemented and are operating effectively. However, certification acknowledges only that controls were appropriate, properly implemented and are operating effectively. Certification does not imply that the residual security risk is acceptable or an approval to operate has been granted.

The purpose of the residual security risk assessment is to assess the risks, controls and residual security risk relating to the operation of a system. In situations where the system is non-conformant, the system owner may have to take corrective actions. The residual risk may not be great enough to preclude a certification authority recommending to the Accreditation Authority that accreditation be awarded but the risk must be acknowledged and appropriate caveats documented.

7.3. Conducting Audits

Objective:	**The effectiveness of information security measures for systems is periodically reviewed and validated**

Objective:	The effectiveness of information security measures for systems is periodically reviewed and validated
Mandatory Control 1:	Prior to undertaking the audit the system owner must approve the system architecture and associated information security documentation
Mandatory Control 2:	The SecPol, SRMP, SecPlan, SOPs and IRP documentation must be reviewed by the auditor to ensure that it is comprehensive and appropriate for the environment the system is to operate within
Mandatory Control 3:	The Information Security Policy (SecPol) must be reviewed by the auditor to ensure that all relevant controls specified in this manual are addressed
Mandatory Control 4:	Prior to undertaking any system testing in support of the certification process, the system owner must implement the controls for the system
Mandatory Control 5:	The implementation of controls must be assessed to determine whether they have been implemented correctly and are operating effectively
Mandatory Control 6:	The auditor must produce a report of compliance for the certification authority outlining areas of non-compliance for a system and any suggested remediation actions
Recommended Control 1:	Agencies should ensure that auditors conducting audits are able to demonstrate independence and are not also the system owner or certification authority
Recommended Control 2:	The system and security architectures should be reviewed by the auditor to ensure that it is based on sound information security principles and meets information security requirements, including the GOBISM

The aim of an audit is to review and assess:

- the risk identification
- design (including the system and security architectures)
- controls selection
- actual implementation and effectiveness of controls for a system
- supporting information security documentation

The outcome of an audit is a report of compliance and control effectiveness for the certification authority outlining areas of non-compliance for a system and any suggested remediation actions.

An audit may be conducted by agency auditors or an independent security organisation.

7.4. Accreditation Framework

Objective:	**Accreditation is the formal authority for a system to operate, and an important element in fundamental information system governance. Accreditation requires risk identification and assessment, selection and implementation of baseline and other appropriate controls and the recognition and acceptance of residual risks relating to the operation of a system. Accreditation relies on the completion of system certification procedures**
Mandatory Control 1:	Agencies must develop an accreditation framework for their agency
Mandatory Control 2:	Agencies must ensure that each of their systems is awarded accreditation
Mandatory Control 3:	Agencies must ensure that that all systems are awarded accreditation before they are used operationally
Mandatory Control 4:	Agencies must ensure that that all systems are awarded accreditation prior to connecting them to any other internal or external system
Mandatory Control 5:	Agencies must ensure that the period between accreditations of each of their systems does not exceed three years
Mandatory Control 6:	Agencies must not operate a system without accreditation or with a lapsed accreditation unless the accreditation authority has granted a dispensation
Recommended Control 1:	Agencies should ensure information security monitoring, logging and auditing is conducted on all accredited systems

The development of an accreditation framework within the agency will ensure that accreditation activities are conducted in a repeatable and consistent manner across the agency and that consistency across government systems is maintained. This requirement is a fundamental part of a robust governance model and provides a sound process to demonstrate good governance of information systems.

Agencies should reaccredit their systems at least every two years. Accreditations should be commenced at least six months before due date to allow sufficient time for the certification and accreditations processes to be completed. Once three years has elapsed between accreditations, the authority to operate the system (the accreditation) will lapse and the agency will need to either reaccredit the system or request a dispensation to operate without accreditation. It should be noted that operating a system without accreditation is considered extremely risky.

7.5. Conducting Accreditations

Objective:	**As a governance good practice, systems are accredited before they are used operationally**
Mandatory Control 1:	All systems must be certified as part of the accreditation process
Mandatory Control 2:	The Accreditation Authority must accept the residual security risk relating to the operation of a system in order to award accreditation

The aim of accreditation is to give formal recognition and acceptance of the residual security risk to a system and information it processes, stores or communicates as part of the agency's governance arrangements.

The outcome of accreditation is an approval to operate issued by the Accreditation Authority to the system owner.

For agencies the Accreditation Authority is the agency head or their delegate. Depending on the circumstances and practices of an agency, the agency head could choose to delegate their authority to multiple senior executives who have the authority to accept security risks for the specific business functions within the agency, for example, the CISO and the system owner.

More information on the delegation of the agency head's authority can be found in Section 6.1 - The Agency Head.

Accreditation is awarded when the systems comply with the GOBISM, the Accreditation Authority understands and accepts the residual security risk relating to the operation of the system and the Accreditation Authority gives formal approval for the system to operate.

In some cases the Accreditation Authority may not accept the residual security risk relating to the operation of the system. This outcome is predominately caused by security risks being insufficiently considered and documented within the SRMP resulting in an inaccurate scoping of security

measures within the SecPlan. In such cases the Accreditation Authority may request that the SRMP and SecPlan be amended and security measures reassessed before accreditation is awarded.

8. Information Security Documentation

8.1. Documentation Fundamentals

Objective:	Information security documentation is produced for systems, to support and demonstrate good governance
Mandatory Control 1:	Agencies must have a Security Policy (SecPol) for their agency. The SecPol is usually sponsored by the Chief Executive and managed by the CISO or Chief Information Officer (CIO). The ITSM should be the custodian of the SecPol
Mandatory Control 2:	Agencies must ensure that every system is covered by a Security Risk Management Plan (SRMP)
Mandatory Control 3:	Agencies mustensure that every system is covered by a Security Plan (SecPlan)
Mandatory Control 4:	Agencies mustensure that Standard Operating Procedures (SOPs) are developed for systems
Mandatory Control 5:	Agencies mustdevelop an Incident Response Plan and supporting procedures
Mandatory Control 6:	Agency personnel must be trained in, and exercise the Incident Response Plan
Mandatory Control 7:	Agencies must ensure that their SecPol, SRMP, SecPlan, SOPs and IRP are appropriately classified
Recommended Control 1:	Agencies shouldcreate and maintain an overarching document describing the agency's documentation framework, including a complete listing of all information security documentation that shows a document hierarchy and defines how each document is related to the other
Recommended Control 2:	Agencies should ensure that their SRMP, SecPlan, SOPs and IRP are logically connected and consistent for each system, other agency systems and with the agency's SecPol
Recommended Control 3:	The SecPol should include an acceptable use policy for any agency technology equipment, systems, resources and data
Recommended Control 4:	All information security documentation should be formally approved and signed off by a person with an appropriate level of seniority and authority
Recommended Control 5:	Agencies should ensure that all high-level information security documentation is approved by the CISO and the agency head or their delegate
Recommended Control 6:	Agencies should ensure that all system-specific documents are reviewed by the ITSM and approved by the system owner

Objective:	Information security documentation is produced for systems, to support and demonstrate good governance
Recommended Control 7:	Agencies should develop a regular schedule for reviewing all information security documentation
Recommended Control 8:	Agencies should ensure that information security documentation is reviewed at least annually with the date of the most recent review being recorded on each document

Information Security Documentation requirements are summarized in the table below.

Title	Abbreviation	Reference
Information Security Policy	SecPol	8.2
Security Risk Management Plan	SRMP	8.3
System Security Plan	SecPlan	8.4
Site Security Plan	SitePlan	11.2
Standard Operating Procedures	SOPs	8.5
Incident Response Plan	IRP	8.6

The implementation of an overarching information security document framework ensures that all documentation is accounted for, complete and maintained appropriately. Furthermore, it can be used to describe linkages between documents, especially when higher level documents are used to avoid repetition of information in lower level documents.

Without appropriate sign-off of information security documentation within an agency, the security personnel will have a reduced ability to ensure appropriate security procedures are selected and implemented. Having sign-off at an appropriate level assists in reducing this security risk as well as ensuring that senior management is aware of information security issues and security risks to the agency's business.

8.2. Information Security Policies (SecPol)

Objective:	Information security policies (SecPol) set the strategic direction for information security
Recommended Control 1:	The Information Security Policy (SecPol) should document the information security, guidelines, standards and responsibilities of an agency
Recommended Control 2:	The Information Security Policy (SecPol) should include topics such as accreditation processes, personnel responsibilities, configuration control, access control, networking and connections with other systems, physical security and media control,

Objective:	Information security policies (SecPol) set the strategic direction for information security
	emergency procedures and information security incident management, change management, and information security awareness and training

The SecPol is an essential part of information security documentation as it outlines the high-level policy objectives. The SecPol can form part of the overall agency security policy.

To provide consistency in approach and documentation, agencies should consider the following when developing their SecPol:

- policy objectives
- how the policy objectives will be achieved
- the guidelines and legal framework under which the policy will operate
- stakeholders
- education and training
- what resourcing will be available to support the implementation of the policy
- what performance measures will be established to ensure that the policy is being implemented effectively
- a review cycle

Agencies should also avoid outlining controls for systems within their SecPol. The controls for a system will be determined by this manual and based on the scope of the system, along with any additional controls as determined by the SRMP, and documented within the SecPlan.

8.3. Security Risk Management Plans (SRMP)

Objective:	Security Risk Management Plans (SRMP) identify security risks and appropriate treatment measures for systems
Recommended Control 1:	Agencies should determine agency and system specific security risks that could warrant additional controls to those specified in this manual
Recommended Control 2:	The Security Risk Management Plan should contain a security risk assessment and a corresponding treatment strategy
Recommended Control 3:	Agencies should incorporate their SRMP into their wider agency risk management plan
Recommended Control 4:	Agencies should develop their SRMP in accordance with international standards for risk management

The SRMP is considered to be a best practice approach to identifying and reducing potential security risks. Depending on the documentation framework chosen, multiple systems can refer to, or build upon, a single SRMP.

SRMPs may be developed on a functional basis, systems basis or project basis. For example, where physical elements will apply to all systems in use within that agency, a single SRMP covering all physical elements is acceptable. Generally each system will require a separate SRMP.

Information on the development of SRMP can be found:

- ISO 27005:2011, Information Security Risk Management
- ISO 22301:2012, Business Continuity

Risks within an agency can be managed if they are not known, and if they are known, failing to treat or accept them is also a failure of risk management. For this reason SRMPs consist of two components, a security risk assessment and a corresponding treatment strategy. If an agency fails to incorporate SRMPs for systems into their wider agency risk management plan, then the agency will be unable to manage risks in a coordinated and consistent manner across the agency.

The International Organization for Standardization has developed an international risk management standard, including principles and guidelines on implementation, outlined in ISO 31000:2009, Risk Management – Principles and Guidance. The terms and definitions for this standard can be found in ISO/IEC Guide 73, Risk Management – Vocabulary – Guidelines. The ISO/IEC 270xx series of standards also provides guidance.

8.4. System Security Plans (SecPlan)

Objective:	**System Security Plans (SecPlan) specify the information security measures for systems**
Mandatory Control 1:	Agencies must select controls from this manual to be included in the SecPlan based on the scope of the system with additional system specific controls being included as a result of the associated SRMP
Recommended Control 1:	Agencies should include a Key Management Plan in the SecPlan

The SecPlan describes the implementation and operation of controls within the system derived from the GOBISM and the SRMP. Depending on the documentation framework chosen, some details common to multiple systems can be consolidated in a higher level SecPlan.

There can be many stakeholders involved in defining a SecPlan, including representatives from the:

- x project, who must deliver the capability (including contractors)
- x owners of the information to be handled
- x system users for whom the capability is being developed
- x management audit authority
- x CISO, ITSM and system owners
- x system certifiers and accreditors
- x information management planning areas
- x infrastructure management

The GOBISM provides a list of controls that are potentially applicable to a system based on its functionality and the technology it is implementing. Agencies will need to determine which controls are in scope of the system and translate those controls to the SecPlan. These controls will then be assessed on their implementation and effectiveness during an information security assessment as part of the accreditation process.

8.5. Standard Operating Procedures (SOP)

Objective:	**Standard Operating Procedures (SOPs) ensure security procedures are followed in an appropriate and repeatable manner**
Recommended Control 1:	Agencies should develop separate SOPs for ITSM, system administrator and system user
Recommended Control 2:	The procedures that should be documented in the ITSM, system administrator and system user‘s SOP are provided in the table below
Recommended Control 3:	ITSMs, system administrators and system users should sign a statement that they have read and agree to abide by their respective SOPs

SOPs provide step-by-step guides to undertaking information security related tasks and processes. They provide assurance that tasks can be undertaken in a secure and repeatable manner, even by system users without strong technical knowledge of the system’s mechanics.

In order to ensure that personnel undertake their duties in an appropriate manner, with a minimum of confusion, it is important that the roles of ITSMs, system administrators and system users are covered by SOPs. Furthermore, taking steps to ensure that SOPs are consistent with SecPlans will reduce the potential for confusion resulting from conflicts in policy and procedures.

The ITSM SOPs are intended to cover the management and leadership of information security functions within the agency.

The system administrator SOPs focus on the administrative activities related to system operations.

The system user SOPs focus on day to day activities that system users need to be made aware of, and comply with, when using systems.

When SOPs are produced the intended audience should be made aware of their existence and acknowledge that they have read, understood and agree to abide by their contents.

Topic	Procedures to be included in the SOPs		
	ITSM	System administrators	System users
Access Control	Authorizing access rights to applications and data	Implementing access rights to applications and data	N/A
Asset Musters	Labelling, registering and mustering assets, including media	N/A	N/A
Audit Logs	Reviewing system audit trails and manual logs, particularly for privileged users	N/A	N/A
Configuration Control	Approving an releasing changes to the system software and configurations	Implementing changes to the system software or configurations	N/A
Information Security Incidents	Detecting, reporting and managing potential information security incidents	Detecting, reporting and managing potential information security incidents	What to do in the case of a suspected or actual information security incident
	Establishing the cause of any information security incident, whether accidental or deliberate	Establishing the cause of any information security incident, whether accidental or deliberate	
	Actions to be taken to recover and minimize the exposure from an information security incident	Actions to be taken to recover and minimize the exposure from an information security incident	
	Additional actions to prevent reoccurrence	Additional actions to prevent reoccurrence	
Data transfers	Managing the review of media	N/A	N/A

Topic	Procedures to be included in the SOPs		
	ITSM	System administrators	System users
	containing classified information that is to be transferred off-site		
	Managing of incoming media for malware or unapproved software		
IT equipment	Managing the disposal and destruction of unserviceable IT equipment and media		N/A
System Patching	Advising and recommending system patches, updates and version changes based on security notices and related advisories	N/A	N/A
	Reviewing system user accounts, system parameters and access controls to ensure that the system is secure		
System integrity audit	Checking the integrity of system software	N/A	N/A
System maintenance	Testing access controls	N/A	N/A
	Managing the ongoing security and functionality of system software (maintaining awareness of current software vulnerabilities, testing and applying software patches/updates/signatures, and applying appropriate hardening techniques)		
User Account Management	Authorizing new system users	Adding and removing system users	N/A
		Setting system user privileges	
		Cleaning up directories and files when a system user departs or changes roles	
System backup and	N/A	Backing up data,	N/A

Topic	Procedures to be included in the SOPs		
	ITSM	System administrators	System users
recovery		including audit logs Securing backup tapes Recovering from system failures	
Acceptable Use	N/A	N/A	Acceptable uses of the system(s)
End of Day	N/A	N/A	How to secure systems at the end of the day
Media Control	N/A	N/A	Procedures for handling and using media
Passwords	N/A	N/A	Choosing and protecting password(s)
Temporary absence	N/A	N/A	How to secure systems when temporarily absent

8.6. Incident Response Plans (IRP)

Objective:	**Incident Response Plans (IRP) outline actions to take in response to an information security incident**
Mandatory Control 1:	Agencies must include, as a minimum, the following content within their IRP: x broad guidelines on what constitutes an information security incident x the minimum level of information security incident response and investigation training for system users and system administrators x the authority responsible for initiating investigations of an information security incident x the steps necessary to ensure the integrity of evidence supporting an information security incident x the steps necessary to ensure that critical systems remain operational x when and how to formally report information security

Objective:	Incident Response Plans (IRP) outline actions to take in response to an information security incident
	incidents x national policy requirements for incident reporting (see Chapter 10 – Information Security Incidents).
Recommended Control 1:	Agencies should include the following content within their IRP: x clear definitions of the types of information security incidents that are likely to be encountered x the expected response to each information security incident type x the authority within the agency that is responsible for responding to information security incidents x the criteria by which the responsible authority would initiate or request formal police investigations of an information security incident x which other agencies or authorities need to be informed in the event of an investigation being undertaken x the details of the system contingency measures or a reference to these details if they are located in a separate document

The purpose of developing an IRP is to ensure that information security incidents are appropriately managed. In most situations the aim of the response will be to contain the incident and prevent the information security incident from escalating. The preservation of any evidence relating to the information security incident for criminal, forensic and process improvement purposes is also an important consideration.

9. Information Security Monitoring

9.1. Information Security Reviews

Objective:	Information security reviews maintain the security of systems and detect gaps and deficiencies
Recommended Control 1:	Agencies should undertake and document information security reviews of their systems at least annually
Recommended Control 2:	Agencies should have information security reviews conducted by personnel independent to the target of the review or by an independent third party
Recommended Control 3:	Agencies should review the components detailed below: x Information security documentation (SecPol. SRMPs, SecPlans, SitePlan, SOPs and IRP) x Dispensations (prior to the identified expiry date) x Operating environment (when an identified threat emerges or changes, an agency gains or loses a function or the operation of functions are moved to a new physical environment) x Procedures (after an information security incident or test exercise) x System security (items that could affect security of the system on a regular basis) x Threats (changes in a risk environment and risk profile) x GOBISM (changes to controls)

Annual reviews of an agency's information security posture can assist with ensuring that agencies are responding to the latest threats, environmental changes and that systems are properly configured in accordance with any changes to information security documentation and guidance.

Incidents, significant changes or an aggregation of minor changes may require a security review to determine and support any necessary changes and to demonstrate good systems governance. An agency may choose to undertake an information security review:

- x as a result of a specific information security incident
- x because a change to a system or its environment that significantly impacts on the agreed and implemented system architecture and information security policy
- x as part of a regular scheduled review

9.2. Vulnerability Analysis

Objective:	Exploitable information system weaknesses can be identified by vulnerability analyses and inform risks to systems
Recommended Control 1:	Agencies should implement a vulnerability analysis strategy by: x monitoring public domain information about new vulnerabilities in operating systems and application software x considering the use of automated tools to perform vulnerability assessments on systems in a controlled manner x running manual checks against system configurations to ensure that only allowed services are active and that disallowed services are prevented x using security checklists for operating systems and common applications x examining any significant incidents on the agency's systems
Recommended Control 2:	Agencies should conduct vulnerability assessments in order to establish a baseline: x before a system is first used x after any significant incident x after a significant change to the system x after changes to standards, policies and guidelines x as specified by an ITSM or the system owner
Recommended Control 3:	Agencies should analyse and treat all vulnerabilities and subsequent security risks to their systems identified during a vulnerability assessment

Vulnerabilities may be unintentionally introduced and new vulnerabilities are constantly identified, presenting ongoing risks to information systems security.

Vulnerabilities may occur as a result of poorly designed or implemented information security practices, accidental activities or malicious activities, and not just as the result of a technical issue.

A baseline or known point of origin is the basis of any comparison and allows measurement of changes and improvements when further information security monitoring activities are conducted.

9.3. Change Management

Objective:	To ensure information security is an integral part of the change management process, it should be incorporated into the agency's IT governance and management activities
Mandatory Control 1:	When a configuration change impacts the security of a system and is subsequently assessed as having changed the overall security risk for the system, the agency must reaccredit the system
Recommended Control 1:	Agencies should ensure that for routine and urgent changes: x the change management process, as defined in the relevant information security documentation, is followed x the proposed change is approved by the relevant authority x any proposed change that could impact the security of a system or accreditation status is submitted to the Accreditation Authority for approval x all associated information security documentation is updated to reflect the change
Recommended Control 2:	Agencies should follow this change management process outline: x produce a written change request x submit the change request to all stakeholders for approval x document the changes to be implemented x test the approved changes x notification to user of the change schedule and likely effect or outage x implement the approved changes after successful testing x update the relevant information security documentation including the SRMP, SecPlan and SOPs x notify and educate system users of the changes that have been implemented as close as possible to the time the change is applied x continually educate system users in regards to changes

The need for change can be identified in various ways, including:

- x system users identifying problems or enhancements
- x vendors notifying of upgrades to software or IT equipment
- x vendors notifying of the end of life to software or IT equipment
- x advances in technology in general
- x implementing new systems that necessitate changes to existing systems
- x identifying new tasks requiring updates or new systems
- x organizational change
- x business process or concept of operation change

- standards evolution
- government policy or Cabinet directives
- threat or vulnerability notification
- other incidents or continuous improvement activities

A proposed change to a system could involve:

- an upgrade to, or introduction of, IT equipment
- an upgrade to, or introduction of, software
- environment or infrastructure change
- major changes to access controls

The accreditation of a system accepts residual security risk relating to the operation of that system. Changes may impact the overall security risk for the system. It is essential that the Accreditation Authority is consulted and accepts the changes and any changes to risk.

9.4. Business Continuity and Disaster Recovery

Objective:	**To ensure business continuity and disaster recovery processes are established to assist in meeting the agency's business requirements, minimize any disruption to the availability of information and systems, and assist recoverability**
Mandatory Control 1:	Agencies must determine availability and recovery requirements for their systems and implement appropriate measures to support them
Recommended Control 1:	Agencies should: - identify vital records - backup all vital records - store backups of critical information, with associated documented recovery procedures, at a remote location secured in accordance with the requirements - test backup and restoration processes regularly to confirm their effectiveness
Recommended Control 2:	Agencies should develop and document a business continuity plan
Recommended Control 3:	Agencies should develop and document a disaster recovery plan

Availability and recovery requirements will vary based on each agency's business needs and are likely to be widely variable across government. Agencies will determine their own availability and recovery requirements and implement appropriate measures to achieve them as part of their risk management and governance processes.

Having a backup strategy in place is a fundamental part of business continuity planning. The backup strategy ensures that critical business information is recoverable if lost. Vital records are defined as any information, systems data, configurations or equipment requirements necessary to restore normal operations.

It is important to develop a business continuity plan to assist in ensuring that critical systems and data functions can be maintained when the system is operating under constraint, for example, when bandwidth is limited.

Developing and documenting a disaster recovery plan will reduce the time between a disaster occurring and critical functions of systems being restored.

10. Information Security Incidents

10.1. Detecting Information Security Incidents

Objective:	**To ensure that appropriate tools, processes and procedures are implemented to detect information security incidents, to minimize impact and as part of the suite of good IT governance activities**
Recommended Control 1:	Agencies should develop, implement and maintain tools and procedures covering the detection of potential information security incidents, incorporating: x counter-measures against malicious code x intrusion detection strategies x data egress monitoring & control x audit analysis x system integrity checking x vulnerability assessments
Recommended Control 2:	Agencies should use the results of the security risk assessment to determine the appropriate balance of resources allocated to prevention versus detection of information security incidents

Processes for the detection of information security incidents will assist in mitigating the most common vectors used to exploit systems.

Many potential information security incidents are noticed by personnel rather than automated or other software tools. Personnel should be well trained and aware of information security issues and indicators of possible information security incidents.

Agencies may consider some of the tools described in the table below for detecting potential information security incidents.

Tool	Description
Network and host Intrusion Detection Systems (IDSs)	Monitor and analyze network and host activity, usually relying on a list of known attack signatures to recognize/ detect malicious activity and potential information security incidents
Anomaly detection systems	Monitor network and host activities that do not conform to normal system activity
Intrusion Prevention Systems (IPS) and Host Based Intrusion Prevention Systems (HIPS)	Some IDs are combined with functionality to counter detected attacks or anomalous activity (IDS/IPS)

System integrity verification and integrity checking	Used to detect changes to critical system components such as files, directories or services. These changes may alert a system administrator to unauthorized changes that could signify an attack on the system and inadvertent system changes that render the system open to attack.
Log analysis	Involves collecting and analyzing event logs using pattern recognition to detect anomalous activities
White Listing	Lists the authorized activities and applications and permits their usage
Black Listing	Lists the non-authorized activities and applications and prevents their usage
Data Loss Prevention (DLP)	Data Egress monitoring and control

10.2. Reporting Information Security Incidents

Objective:	**Reporting information security incidents, assists in maintaining an accurate threat environment picture for government systems**
Mandatory Control 1:	Agencies must direct personnel to report information security incidents to an ITSM as soon as possible after the information security incident is discovered in accordance with agency procedures
Mandatory Control 2:	The ITSM must keep the CISO fully informed of information security incidents within an agency
Mandatory Control 3:	The Agency ITSM must report significant information security incidents to the BCC
Mandatory Control 4:	Agencies that outsource their information technology services and functions must ensure that the service provider consults with the agency when an information security incident occurs
Recommended Control 1:	Agencies should: x encourage personnel to note and report any observed or suspected security weaknesses in, or threats to, systems or services x establish and follow procedures for reporting software malfunctions x put mechanisms in place to enable the types, volumes and costs of information security incidents and malfunctions to be quantified and monitored x deal with the violation of agency information security policies and procedures by personnel through a formal disciplinary process
Recommended Control 2:	Agencies should formally report information security incidents

Objective:	Reporting information security incidents, assists in maintaining an accurate threat environment picture for government systems
	using IODEF standard.

The requirement to lodge an information security incident report still applies when an agency has outsourced some or all of its information technology functions and services.

The CISO is required to keep the CSO and/or Agency Head informed of information security incidents within their agency. The ITSM actively manages information security incidents and must ensure the CISO has sufficient awareness of and information on any information security incidents within an agency.

Reporting on low-level incidents can be adequately managed through periodic (at least monthly) reports. Serious incidents will require more immediate attention.

Significant information security incidents must be reported to BCC. The BCC uses these reports as the basis for identifying and responding to information security events across government, for developing new policy, procedures, techniques and training measures to prevent the recurrence of similar information security incidents across government.

Reporting of information security incidents to the BCC through the appropriate channels ensures that appropriate and timely assistance can be provided to the agency. In addition, it allows the BCC to maintain an accurate threat environment picture for government systems.

In the case of outsourcing of information technology services and functions, the agency is still responsible for the reporting of all information security incidents. As such, the agency must ensure that the service provider informs them of all information security incidents to allow them to formally report these to the BCC.

10.3. Managing Information Security Incidents

Objective:	To identify and implement processes for incident analysis and selection of appropriate remedies which will assist in preventing future information security incidents
Mandatory Control 1:	Agencies must detail information security incident responsibilities and procedures for each system in the relevant SecPlan, SOPs and IRP
Mandatory Control 2:	Agencies must follow IODEF Standard and should include the following information in their register: x the date the information security incident was discovered x the date the information security incident occurred

Objective:	To identify and implement processes for incident analysis and selection of appropriate remedies which will assist in preventing future information security incidents
	x a description of the information security incident, including the personnel, systems and locations involved x the action taken x to whom the information security incident was reported x the file reference
Mandatory Control 3:	Agencies must implement procedures and processes to detect data spills. Agency SOPs must include procedure for: x all personnel with access to systems x notification to the ITSM of any data spillage x notification to the ITSM of access to any data which they are not authorised to access
Mandatory Control 4:	Agencies must document procedures for dealing with data spills in their IRP
Mandatory Control 5:	Agencies must treat any data spill as an information security incident and follow the IRP to deal with it
Mandatory Control 6:	When a data spill occurs agencies must report the details of the data spill to the information owner
Recommended Control 1:	Agencies should ensure that all information security incidents are recorded in a register
Recommended Control 2:	Agencies should follow the steps described below when malicious code is detected: x isolate the infected system x decide whether to request assistance from BCC x if such assistance is requested and agreed to, delay any further action until advised BCC x scan all previously connected systems and any media used within a set period leading up to the information security incident, for malicious code x isolate all infected systems and media to prevent reinfection x change all passwords and key material stored or potentially accessed from compromised systems, including any websites with password controlled access x advise system users of any relevant aspects of the compromise, including a recommendation to change all passwords on compromised systems x use up-to-date antivirus software to remove the infection from the systems or media x monitor network traffic for malicious activity

Objective:	To identify and implement processes for incident analysis and selection of appropriate remedies which will assist in preventing future information security incidents
	x report the information security incident and perform any other activities specified in the IRP x in the worst case scenario, rebuild and reinitialize the system
Recommended Control 3:	For evidence gathering, agencies should: x transfer a copy of raw audit trails and other relevant data onto media for secure archiving, as well as securing manual log records for retention x ensure that all personnel involved in the investigation maintain a record of actions undertaken to support the investigation

Ensuring that system users are aware of reporting procedures will assist in identifying any information security incidents that an ITSM, or system owner fail to notice.

The purpose of recording information security incidents within a register is to highlight the nature and frequency of information security incidents so that corrective action can be taken. This information can subsequently be used as an input into future security risk assessments of systems.

A data spill is defined as the unauthorized or unintentional release, transmission or transfer of data.

The guidance for handling malicious code infections is provided to assist in preventing the spread of the infection and to prevent reinfection. Important details include:

- x the infection date of the machine
- x the possibility that system records and logs could be compromised
- x the period of infection

A complete operating system reinstallation, or an extensive comparison of checksums or other characterization information, is the only reliable way to ensure that malicious code is eradicated.

While gathering evidence it is important to maintain the integrity of the information and the chain of evidence. Even though in most cases an investigation does not directly lead to a police prosecution, it is important that the integrity of evidence such as manual logs, automatic audit trails and intrusion detection tool outputs be protected.

11. Physical Security

11.1. Facilities

Objective:	Physical security measures are applied to facilities protect systems and their infrastructure
Mandatory Control 1:	Agencies must ensure that any facility containing a system or its associated infrastructure, including deployable systems, are certified and accredited in accordance with the Physical Security Requirements

The certification of an agency's physical security measures is an essential part of the certification and accreditation process. High Level information relating to physical security is contained in ISO/IEC 27002:2013.

The application of defense-in-depth to the protection of systems and infrastructure is enhanced through the use of successive layers of physical security. Typically the layers of security are:

- site
- building
- room
- racks
- approved containers
- operational hours.

All layers are designed to control and limit access to those with the appropriate authorization for the site, infrastructure and system. Deployable platforms need to meet physical security certification requirements as with any other system. Physical security certification authorities dealing with deployable platforms may have specific requirements that supersede the requirements of this manual and as such security personnel should contact their appropriate physical security certification authority to seek guidance.

11.2. Servers and Network Devices

Objective:	Secured server and communications rooms provide appropriate physical security for servers and network devices
Mandatory Control 1:	Agencies must ensure that servers and network devices are secured within cabinets as outlined by GOB
Mandatory Control 2:	Agencies must ensure that keys or equivalent access mechanisms to server rooms, communications rooms and security containers

Objective:	Secured server and communications rooms provide appropriate physical security for servers and network devices
	are appropriately controlled
Mandatory Control 3:	Agencies must notleave server rooms, communications rooms or security containers in an unsecured state unless the server room is occupied by authorised personnel
Mandatory Control 4:	Agencies must develop a Site Security Plan (SitePlan) for each server and communications room. Information to be covered includes, but is not limited to: x a summary of the security risk review for the facility the server or communications room is located in x roles and responsibilities of facility and security personnel x the administration, operation and maintenance of the electronic access control system or security alarm system x key management, the enrolment and removal of system users and issuing of personal identification number codes and passwords x regular inspection of the generated audit trails and logs x end of day checks and lockup x reporting of information security incidents x what activities to undertake in response to security alarms
Recommended Control 1:	Agencies should use a secured server or communications room within a secured facility

Site security plans (SitePlan), the physical security equivalent of the SecPlan and SOPs for systems, are used to document all aspects of physical security for systems. Formally documenting this information ensures that standards, controls and procedures can easily be reviewed by security personnel.

11.3. Network Infrastructure

Objective:	Network infrastructure is protected by secure facilities
Recommended Control 1:	Agencies should locate patch panels, fiber distribution panels and structured wiring enclosures within at least lockable commercial cabinets

Network infrastructure is considered to process information being communicated across it.

It is important to note that physical controls do not provide any protection against malicious software or other malicious entities that may be residing on or have access to the system.

In order to prevent tampering with patch panels, fiber distribution panels and structured wiring, any such enclosures need to be placed within at least lockable commercial cabinets. Furthermore, keys for such cabinets should not be remain in locks as this defeats the purpose of using lockable commercial cabinets in the first place.

11.4. IT Equipment

Objective:	**IT equipment is secured outside of normal working hours, is non-operational or when work areas are unoccupied**
Mandatory Control 1:	Agencies must account for all IT equipment containing media

IT equipment containing medias includes but is not limited to workstations, printers, photocopiers, scanners and multi-function devices (MFDs).

Additional information relating to IT equipment and media can be found in the following chapters and sections of this manual:

- Section 14.1 - Fax Machines, Multifunction Devices and Network Printers
- Chapter 15 - Product Security
- Chapter 16 – Decommissioning and Disposal

Ensuring that IT equipment containing media is accounted for by using asset registers, equipment registers, operational & configuration records and regular audits will assist in preventing loss or theft, or in the cases of loss or theft, alerting appropriate authorities to its loss or theft.

Asset registers may not provide a complete record as financial limits may result in smaller value items not being recorded. In such cases other registers and operational information can be utilized to assist in building a more complete record.

11.5. Tamper Evident Seals

Objective:	**Tamper evident seals and associated auditing processes identify attempts to bypass the physical security of systems and their infrastructure**
Recommended Control 1:	Agencies should record the usage of seals in a register that is appropriately secured

Objective:	Tamper evident seals and associated auditing processes identify attempts to bypass the physical security of systems and their infrastructure
Recommended Control 2:	Agencies should record in a register, information on: x issue and usage details of seals and associated tools x serial numbers of all seals x the location or asset on which each seal for is used
Recommended Control 3:	Agencies shouldconsult with the seal manufacturer to ensure that, if available, any purchased seals and sealing tools display a unique identifier or image appropriate to the agency
Recommended Control 4:	Seals and any seal application tools should be secured when not in use
Recommended Control 5:	Agencies should notallow contractors to independently purchase seals and associated tools on behalf of the government
Recommended Control 6:	Agencies should review seals for differences with a register at least annually. At the same time seals should be examined for any evidence of tampering

Recording information about seals in a register and on which asset they are used assists in reducing the security risk that seals could be substituted without security personnel being aware of the change.

Using uniquely numbered seals ensures that a seal can be uniquely mapped to an asset. This assists security personnel in reducing the security risk that seals could be replaced without anyone being aware of the change.

Users of assets with seals should be encouraged to randomly check the integrity of the seals and to report any concerns to security personnel. In addition, conducting at least annual reviews will allow for detection of any tampering to an asset and ensure that the correct seal is located on the correct asset.

12. Personnel Security

12.1. Information Security Awareness and Training

Objective:	**A security culture is fostered through induction training and ongoing security education tailored to roles, responsibilities, changing threat environment and sensitivity of information, systems and operations**
Mandatory Control 1:	Agency management must ensure that all personnel who have access to a system have sufficient information security awareness and training
Mandatory Control 2:	Agencies must provide ongoing information security awareness and training for personnel on topics such as responsibilities, legislation and regulation, consequences of non-compliance with information security policies and procedures, and potential security risks and counter-measures, including information on: X any legislative or regulatory mandates and requirements X any national or agency policy mandates and requirements X agency security appointments and contacts X the legitimate use of system accounts and software X the security of accounts, including shared passwords X authorisation requirements for applications, databases and data X the security risks associated with non-agency systems, particularly the Internet X reporting any suspected compromises or anomalies X reporting requirements for information security incidents, suspected compromises or anomalies X protecting workstations from unauthorised access X informing the support section when access to a system is no longer needed X observing rules and regulations governing the secure operation and authorised use of systems X supporting documentation such as SOPs and user guides
Mandatory Control 3:	Agencies must provide information security awareness training as part of their employee induction programmes
Recommended Control 1:	Agencies should ensure that information security awareness and training includes advice to system users not to attempt to: X tamper with the system X bypass, strain or test information security mechanisms

Objective:	A security culture is fostered through induction training and ongoing security education tailored to roles, responsibilities, changing threat environment and sensitivity of information, systems and operations
	x introduce or use unauthorized IT equipment or software on a system x replace items such as keyboards, pointing devices and other peripherals with personal equipment x assume the roles and privileges of others x relocate equipment without proper authorization

Agency management is responsible for ensuring that an appropriate information security awareness and training program is provided to personnel. Without management support, security personnel might not have sufficient resources to facilitate awareness and training for other personnel.

Awareness and knowledge degrades over time without ongoing refresher training and updates. Providing ongoing information security awareness and training will assist in keeping personnel aware of issues and their responsibilities.

Methods that can be used to continually promote awareness include logon banners, system access forms and departmental bulletins and memoranda.

Information security awareness and training programs are designed to help system users:

- x become familiar with their roles and responsibilities
- x understand any legislative or regulatory mandates and requirements
- x understand any national or agency policy mandates and requirements
- x understand and support security requirements
- x assist in maintaining security
- x learn how to fulfil their security responsibilities

As part of the guidance provided to system users, there should be sufficient emphasis placed on the activities that are not allowed on systems. The minimum list of content will also ensure that personnel are sufficiently exposed to issues that could cause an information security incident through lack of awareness or through lack of knowledge.

12.2. Authorizations and Briefings

Objective:	Only appropriately authorized, cleared and briefed personnel are allowed access to systems
Mandatory Control 1:	Agencies must specify in the System Security Plan (SecPlan) any authorisations and briefings necessary for system access
Mandatory Control 2:	Where systems process, store or communicate unprotected GOB information, agencies must not allow foreign nationals, including seconded foreign nationals, to have access to the system
Recommended Control 1:	Agencies should: x limit system access on a need-to-know/need to access basis x provide system users with the least amount of privileges needed to undertake their duties x have any requests for access to a system authorized by the supervisor or manager of the system user
Recommended Control 2:	Agencies should maintain a secure record of: x all authorized system users x their user identification x why access is required x role and privilege level x who provided the authorization to access the system x when the authorization was granted x maintain the record, for the life of the system or the length of employment whichever is the longer, to which access is granted

Ensuring that the requirements for access to a system are documented and agreed upon will assist in determining if system users have appropriate authorizations and need-to-know to access the system. Access requirements that will need to be documented include general users, privileged users, systems administrators, contractors and visitors.

Personnel seeking access to a system will need to have a genuine business requirement to access the system as verified by their supervisor or manager. Once a requirement to access a system is established, the system user should be given only the privileges that they need to undertake their duties. Providing all system users with privileged access when there is no such requirement can cause significant security vulnerabilities in a system.

In many cases, the requirement to maintain a secure record of all personnel authorized to access a system, their user identification, who provided the authorization and when the authorization was granted, can be met by retaining a completed system account request form signed by the supervisor or manager of the system user.

12.3. Using the Internet

Objective:	Personnel use Internet services in a responsible and security conscious manner, consistent with agency policies
Mandatory Control 1:	Agencies must make their system users aware of the agency's Web usage policies and personnel must formally acknowledge and accept agency Web usage policies
Mandatory Control 2:	Agencies must ensure personnel are instructed to take special care when posting information on the Web
Mandatory Control 3:	Agencies must ensure personnel posting information on the Web maintain separate professional accounts from any personal accounts they have for websites
Recommended Control 1:	Accessing personal accounts from agency systems should be discouraged
Recommended Control 2:	Agencies should notallow personnel to use peer-to-peer applications over the Internet
Recommended Control 3:	Agencies should notallow personnel to receive files via peer-to-peer, IM or IRC applications

This section covers information relating to personnel using Internet services such as the Web, Web-based email, news feeds, subscriptions and other services.

Users mustbe familiar with and formally acknowledge agency Web usage policies for system users in order to follow the policy and guidance.

Personnel need to take special care not to accidentally post information on the Web, especially in forums and blogs. Even unclassified information that appears to be benign in isolation could, in aggregate, have a considerable security impact on the agency, government sector or wider government.

To ensure that personal opinions of agency personnel are not interpreted as official policy or associated with an agency, personnel will need to maintain separate professional and personal accounts when using websites, especially when using online social networks. Accessing personal accounts from an agency's systems is discouraged.

Personnel using peer-to-peer file sharing applications are often unaware of the extent of files that are being shared from their workstation. In most cases peer-to-peer file sharing applications will scan workstations for common file types and share them automatically for sharing or public consumption. Examples of peer-to-peer file sharing applications include Shareaza, KaZaA, Ares, Limewire, eMule and uTorrent. When personnel receive files via peer-to-peer file sharing, IM or IRC applications they are often bypassing security mechanisms put in place by the agency to detect and

quarantine malicious code. Personnel should be encouraged to send files via established methods such as email, to ensure they are appropriately scanned for malicious code.

13. Infrastructure

13.1. Cable Management Fundamentals

Objective	Cable management systems are implemented to allow easy integration of systems across government and minimize the opportunity for tampering or unauthorized change
Recommended Control 01:	Agencies should use fiber optic cable for backbone infrastructures and installations
Recommended Control 02:	Agencies should use fiber optic cabling
Recommended Control 03:	Agencies should not use fiber optic cable incorporating conductive metal strengtheners or sheaths except where essential for cable integrity

The design of a backbone requires consideration of a number of criteria including the capacity of the cable to carry the predicted volume of data at acceptable speeds. An element of "future proofing" is also required as re-cabling to manage capacity issues can be costly. Fiber optic cable provides a convenient means of securing and "future proofing" backbones.

Fiber optic cable is considered more secure than copper cables and provides electrical isolation of signals. Fiber will also provide higher bandwidth and speed to allow a degree of future-proofing in network design.

13.2. Cable Management for Non-Shared Government Facilities

Objective	Cable management systems in non-shared government facilities are implemented in a secure and easily inspectable and maintainable way
Recommended Control 01:	Cabling shouldbe inspectable at a minimum of five-meter intervals

Regular inspections of cable installations are necessary to detect any unauthorized or malicious tampering or cable degradation in non-shared government facilities.

13.3. Cable Management for Shared Government Facilities

Objective	Cable management systems in shared government facilities are

	implemented in a secure and easily inspectable and maintainable way
Recommended Control 01:	Agencies should use fiber optic cabling
Recommended Control 02:	Cabling should be inspectable at a minimum of five-meter intervals
Recommended Control 03:	Approved cable groups may share a common reticulation system but shouldhave either a dividing partition or a visible gap between the differing cable groups or bundles
Recommended Control 04:	Flexible or plastic conduit should be used in walls to run cabling from cable trays to wall outlets
Recommended Control 05:	Approved cable groups should have either a dividing partition or a visible gap between the individual cable groups. If the partition or gap exists, cable groups may share a common reticulation system
Recommended Control 06:	Cabling from cable trays to wall outlets should run in flexible or plastic conduit
Recommended Control 07:	Power filters should be used to provide a filtered power supply and reduce opportunity for technical attacks

Fiber optic cabling is essential in a shared non-government facility. Fiber optic cabling does not produce and is not influenced by electromagnetic emanations; as such it offers the highest degree of protection from electromagnetic emanation effects especially in a shared facility where one agency does not have total control over other areas of the facility.

Many more fibers can be run per cable diameter than wired cables thereby reducing cable infrastructure costs as well. Fiber cable is the best method to future proof against unforeseen threats.

In a shared facility it is important that cabling systems are inspected for illicit tampering and damage on a regular basis and have stricter controls than a non-shared facility. In a shared facility with another government agency, tighter controls may be required for sharing reticulation systems.

In a shared facility with another government agency, cabling must be laid correctly in walls allowing neater installations while maintaining separation and inspectability requirements.

Power filters are used to provide a filtered (clean) power supply and reduce opportunity for technical attacks.

13.4. Cable Management for Shared Non-Government Facilities

Objective	**Cable management systems are implemented in shared non-government facilities to minimize risks to data and information**

Recommended Control 01:	In a shared Non-Government Facility agencies should use fiber optic cabling
Recommended Control 02:	Cabling shouldbe inspectable at a minimum of five-meter intervals
Recommended Control 03:	Flexible or plastic conduit should be used in walls to run cabling from cable trays to wall outlets
Recommended Control 04:	The front covers of conduits, ducts and cable trays in floors, ceilings and of associated fittings should be clear plastic or be inspectable and have tamper proof seals fitted
Recommended Control 05:	Conduit joints should be sealed with glue or sealant

Fiber optic cabling is essential in a shared non-government facility. Fiber optic cabling does not produce and is not influenced by electromagnetic emanations; as such it offers the highest degree of protection from electromagnetic emanation effects especially in a shared non-government facility where an agency's controls may have a limited effect outside the agency controlled area. Fiber optic cable is more difficult to tap than copper cabling and anti-tampering monitoring can be employed to detect tampering. Many more fibers can be run per cable diameter than wired cables, reducing cable infrastructure costs.

In a shared non-government facility, it is imperative that cabling systems be inspectable for tampering and damage on a regular basis particularly where higher threat levels exist or where threats are unknown.

In a shared non-government facility, cabling run correctly in walls allows for neater installations facilitating separation and inspectability. Controls are more stringent than in a non-shared facility or a shared government facility.

13.5. Cable Labelling and Registration

Objective	**To facilitate cable management, and identify unauthorized additions or tampering**
Recommended Control 01:	The SOPs[6] should record the site conventions for labelling and registration
Recommended Control 02:	Agencies should label cables at each end, with sufficient information to enable the physical identification and inspection of the cable
Recommended Control 03:	Agencies should maintain a register of cables
Recommended Control 04:	The cable register should record at least the following information:

[6] SOP: Standard operating procedure

	x cable identification number x classification x socket number, equipment type, source or destination site/floor plan diagram x seal numbers if applicable
Recommended Control 05:	Agencies should inspect cables for inconsistencies with the cable register in accordance with the frequency defined in the SecPlan[7]

Recording labelling conventions in SOPs facilitates maintenance and fault finding.

Labelling cables with the correct socket number, equipment type, source or destination minimizes the likelihood of improperly cross connecting equipment and can assist in fault finding and configuration management.

Cable registers provide a source of information that assessors can view to verify compliance. Cable registers allow installers and assessors to trace cabling for inspection, tampering or accidental damage. It tracks all cable management changes through the life of the system. Regular cable inspections, are a method of checking the cable management system against the cable register as well as detecting tampering, damage, breakages or other anomalies.

[7]SecPlan: Systems Security Plans

14. Communication Systems and Devices

14.1. Fax Machines, Multifunction Devices and Network Printers

Objective:	Fax machines, multifunction devices (MFD's) and network printers are used in a secure manner
Mandatory Control 1:	Agencies must develop a policy governing the use of fax machines, MFDs, and network printers
Mandatory Control 2:	Where MFDs connected to computer networks have the ability to communicate via a gateway to another network, agencies must ensure that: x each MFD applies user identification, authentication and audit functions for all information communicated by that device x these mechanisms are of similar strength to those specified for workstations on that network x each gateway can identify and filter information in accordance with the requirements for the export of data through a gateway
Recommended Control 1:	Agencies should not enable a direct connection from a MFD to a telephone network unless the telephone network is accredited to the same level as the computer network to which the device is connected
Recommended Control 2:	Any storage devices, drums or other components that may contain data or copies of documents should be disposed of following the processes prescribed in Chapter 16 - Decommissioning and Disposal

This section covers information relating to fax machines, MFDs and network printers connected to either the ISDN, PSTN, HGCE or other networks.

Fax machines, MFDs and network printers are capable of communicating information, and are a potential source of information security incidents. It is therefore essential that agencies develop a policy governing their use.

When a MFD is connected to a computer network and a telephone network the device can act as a bridge between the networks. As such the telephone network needs to be accredited to the same classification as the computer network the MFD is connected to.

As network connected MFDs are considered to be devices that reside on a computer network they need to be able to process the same level of information that the network is capable of processing.

The use of storage media and the characteristics of electrostatic drums allow the recovery of information from such devices and components. To protect the information, prescribed disposal procedures should be followed.

15. Product Security

15.1. Product Selection and Acquisition

Objective:	Products providing security functions for the protection of information are evaluated in order to provide a degree of assurance over the integrity and performance of the product
Recommended Control 1:	Agencies should: x obtain software from verifiable sources and verify its integrity using vendor supplied checksums x validate the software's interaction with the operating systems and network within a test environment prior to use on operational systems
Recommended Control 2:	Agencies should ensure that leasing agreements for IT equipment takes into account the: x difficulties that could be encountered when the equipment needs maintenance x control of remote maintenance, software updates and fault diagnosis x if the equipment can be easily sanitized prior to its return x the possible requirement for destruction if sanitization cannot be performed
Recommended Control 3:	Agencies should choose products from developers that have made a commitment to the ongoing maintenance of the assurance of their product.

Software downloaded from websites on the Internet can contain malicious code or malicious content that is installed along with the legitimate software. Agencies need to confirm the integrity of the software they are installing before deploying it on a system to ensure that no unintended software is installed at the same time.

Agencies should consider security and policy requirements when entering into a leasing agreement for IT equipment in order to avoid potential information security incidents during maintenance, repairs or disposal processes.

Developers that have demonstrated a commitment to ongoing maintenance or evaluation are more likely to be responsive to ensuring that security patches are independently assessed.

15.2. Product Patching and Updating

Objective:	To ensure security patches are applied in a timely fashion to manage software and firmware corrections, vulnerabilities and performance risks
Mandatory Control 1:	Agencies must ensure that any firmware updates are performed in a manner that verifies the integrity and authenticity of the source and of the updating process
Recommended Control 1:	Agencies should monitor relevant sources for information about new vulnerabilities and security patches for software and IT equipment used by the agency
Recommended Control 2:	Where known vulnerabilities cannot be patched, or security patches are not available, agencies should implement: x controls to resolve the vulnerability such as: disable the functionality associated with the vulnerability though product configuration ask the vendor for an alternative method of managing the vulnerability install a version of the product that does not have the identified vulnerability install a different product with a more responsive vendor engage a software developer to correct the software x controls to prevent exploitation of the vulnerability including: apply external input sanitization (if an input triggers the exploit) apply filtering or verification on the software output (if the exploit relates to an information disclosure) apply additional access controls that prevent access to the vulnerability configure firewall rules to limit access to the vulnerable software x controls to contain the exploit including: apply firewall rules limiting outward traffic that is likely in the event of an exploitation apply mandatory access control preventing the execution of

	exploitation code set file system permissions preventing exploitation code from being written to disk white and blacklisting to prevent code execution x controls to detect attacks including: deploy an IDS monitor logging alerts use other mechanisms as appropriate for the detection of exploits using the known vulnerability x controls to prevent attacks including: deploy an IPS or HIPS use other mechanisms as appropriate for the diversion of exploits using the known vulnerability, such as honey pots and null routers.
Recommended Control 3:	Agencies should assess the security risk of using software or IT equipment when a cessation date for support is announced or when the product is no longer supported by the developer

It is important that agencies monitor relevant sources for information about new vulnerabilities and security patches. This way, agencies can take pro-active steps to address vulnerabilities in their systems.

When a security patch is not available for a known vulnerability, there are a number of approaches to reducing the risk to a system. This includes resolving the vulnerability through alternative means, preventing exploitation of the vulnerability, containing the exploit or implementing measures to detect attacks attempting to exploit the vulnerability.

As firmware provides the underlying functionality for hardware it is essential that the integrity of any firmware images or updates are maintained.

Once a cessation date for support is announced for software or IT equipment, agencies will increasingly find it difficult to protect against vulnerabilities found in the software or IT equipment as no security patches will be made available by the manufacturer. Once a cessation date for support is announced agencies should investigate new solutions that will be appropriately supported and establish a plan to implement the new solution.

15.3. Product Sanitization and Disposals

Objective:	IT equipment is sanitized and disposed of in an approved manner
Mandatory Control 1:	Agencies must sanitise or destroy IT equipment containing media before disposal
Mandatory Control 2:	Agencies must formally sanitise and then authorise the disposal of IT equipment, or waste, into the public domain

In order to prevent the disclosure of government information into the public domain, agencies will need to ensure that IT equipment is either sanitized or destroyed before authorized for released into the public domain.

16. Decommissioning and Disposal

16.1. System Decommissioning

Objective:	To ensure systems are safely decommissioned and that software, system logic and data are properly transitioned to new systems or archived in accordance with agency, legal and statutory requirements
Recommended Control 1:	When the Information System reaches the end of its service life in an organization, policy and procedures should be in place to ensure secure decommissioning and transfer or disposal, in order to satisfy corporate, legal and statutory requirements
Recommended Control 2:	Agencies should undertake a risk assessment with consideration given to proportionality in respect of scale and impact of the processes, data, users and licenses system and service to be migrated or decommissioned
Recommended Control 3:	The risk assessment should include the following elements: x Evaluation of the applications inventory and identification of any redundancies x Identification of data owners and key stakeholders x Identification of types of information (Active or Inactive) processed and stored x Identification of software and other (including non-transferable) licenses x Identification of access rights to be transferred or cancelled x Consideration of short and long term reporting requirements x Assessment of equipment and hardware for redeployment or disposal x User re-training
Recommended Control 4:	Agencies should identify relevant service and legal agreements and arrange for their termination
Recommended Control 5:	The decommissioning plan will be based on the migration plan and should incorporate the following elements: x An impact analysis x Issue of notification to service providers, users and customers x Issue of notification of decommissioning to all relevant interfaces and interconnections x Timeframe, plan and schedule

	x Data integrity and validation checks before archiving x Transfer or redeployment of equipment and other assets x Transfer or cancellation of licenses x Removal of redundant equipment and software x Removal of redundant cables and termination equipment x Updates to systems configurations (switches, firewalls etc.) x Equipment and media sanitization (discussed later in this chapter) x Equipment and media disposal (discussed later in this chapter) x Any legal considerations for supply or service contract terminations x Asset register updates x Retraining for, or redeployment of, support staff
Recommended Control 6:	Agencies should identify data retention policies, regulation and legislation
Recommended Control 7:	Agencies should ensure adequate system documentation is archived
Recommended Control 8:	Agencies should archive essential software, system logic, and other system data to allow information to be recovered from archive to ensure adequate system documentation is archived
Recommended Control 9:	The Agency's Accreditation Authority should confirm IA compliance on decommissioning and disposal
Recommended Control 10:	The Agency's Accreditation Authority should confirm asset register updates

System decommissioning is the retirement or termination of a system and its operations

A system decommissioning will have the one or more of the following characteristics:

- x Ending a capability completely i.e. no migration, redevelopment or new version of a capability occurs
- x Combining parts of existing capabilities services into a new, different system
- x As part of wider redesign, where a capability is no longer provided and is decommissioned or merged with other capabilities or systems

Information systems are often supported by service and supply contracts and may also be subject to obligations to provide a service, capability or information. Decommissioning of a system will require the termination of these contracts and service obligations.

An agency policy shall provide a comprehensive approach to system decommissioning from the inception of a system, thus facilitating the termination of supply contracts and service obligations while managing any risks to the Agency.

Security requires a structured approach to decommissioning in order to cease information system operations in a planned, orderly and secure manner. It is also important that the approach for decommissioning systems is consistent and coordinated. Sanitization is important to eliminate any remnant data that could be retrieved by unauthorized parties. These procedures include the following:

- A migration plan;
- A decommissioning plan;
- Archiving;
- Safe disposal of equipment and media; and
- Audit and final signoff.

Once the decision to decommission a system has been taken, it is important to migrate processes, data, users and licenses to replacement systems or to cease activities in an orderly fashion. It is also important to carefully plan the decommissioning process in order to avoid disruption to other systems, ensure business continuity, ensure security, protect privacy and meet any archive and other regulatory and legislative requirements. The basis of a decommissioning plan is a risk assessment.

The decommissioning of a system can be a complex process. A decommissioning plan is an important tool in properly managing the safe decommissioning of a system and in providing reasonable assurance that due process and agency policy has been followed.

Availability and integrity requirements in respect of information may persist for legal and other statutory or compliance reasons and require transfer to other ownership or custodianship for archive purposes. This will also require assurance that the data can continue to be accessed when required (availability) and assurance that it remains unchanged (integrity).

To comply with governance, asset management and audit requirements, the Agency's Accreditation Authority will certify that appropriate processes have been followed. This demonstrates good governance and avoids privacy breaches.

16.2. Media Usage

Objective:	**Media is used with systems in a controlled and accountable manner**

Mandatory Control 1:	Agencies must disable any automatic execution features within operating systems for connectable devices and media
Mandatory Control 2:	Agencies must prevent unauthorized media from connecting to a system via the use of: x device access control software x seals x physical means or x other methods approved by the Accreditation Authority
Recommended Control 1:	Agencies should disable IEEE 1394 interfaces

Some operating systems provide functionality to automatically execute or read certain types of programs that reside on optical media and flash memory media when connected. Automatic loading of a graphical user interface for the system user to browse the contents of the media or installation of software residing on the media can be used for malicious purposes. Using device access control software will prevent unauthorized media from being attached to a system. Using a whitelisting approach allows security personnel greater control over what can, and what cannot, be connected to the system.

Known vulnerabilities have been demonstrated where attackers can connect a FireWire capable device to a locked workstation and modify information in RAM to gain access to encryption keys. As FireWire provides direct access to the system memory, an attacker can read or write directly to memory. The best defense against this vulnerability is to disable access to FireWire ports using either software controls or physically disabling the FireWire ports so that devices cannot be connected. Alternatively select equipment without FireWire capability.

16.3. Media Sanitization

Objective:	**Media that is to be redeployed or is no longer required is sanitized**
Mandatory Control 1:	Agenciesmust document procedures for the sanitisation of media
Mandatory Control 2:	Agencies must destroy the following media types prior to disposal, as they cannot be effectively sanitised: x microfiche x microfilm x optical discs x printer ribbons and the impact surface facing the platen x programmable read-only memory (PROM, EPROM, EEPROM) x flash memory and solid state or hybrid data storage devices x read-only memory x faulty media that cannot be successfully sanitised

Mandatory Control 3:	Agencies must sanitise volatile media by: x overwriting all locations of the media with an arbitrary pattern x followed by a read back for verification x removing power from the media for at least 10 minutes
Mandatory Control 4:	Agencies must sanitise non-volatile magnetic media by: x if pre-2001 or under 15GB: overwriting the media at least three times in its entirety with an arbitrary pattern followed by a read back for verification; or x if post-2001 or over 15GB: overwriting the media at least once in its entirety with an arbitrary pattern followed by a read back for verification

Sanitization is defined as the process of removal of data and information from the storage device such that data recovery using any known technique or analysis is prevented or made unfeasible. The process includes the removal of all useful data from the storage device, including metadata, as well as the removal of all labels, markings, classifications and activity logs.

16.4. Media Destruction

Objective:	**Media that cannot be sanitized is destroyed before disposal**
Mandatory Control 1:	Agencies must document procedures for the destruction of media
Mandatory Control 2:	To destroy media, agencies must: x break up the media x heat the media until it has either burnt to ash or melted; or x degauss the media and then physically destroy the media
Mandatory Control 3:	Agencies must perform the destruction of media under the supervision of at least one person
Mandatory Control 4:	Personnel supervising the destruction of media must: x supervise the handling of the media to the point of destruction and x ensure that the destruction is completed successfully
Recommended Control 1:	The Destruction Register should record: x Date of destruction x Operator and witness x Media type, characteristics and serial number
Recommended Control 2:	Agencies should sanitize media prior to transporting it to an offsite location for destruction

17. Software Security

17.1. Standard Operating Environments

Objective	Standard Operating Environments (SOE) are hardened in order to minimize known vulnerabilities and attack vectors
Mandatory Control 01:	Agencies must ensure that for all servers and workstations: x a technical specification is agreed for each platform with specified controls x a standard configuration created and updated for each operating system type and version x system users do not have the ability to install or disable software without approval x installed software and operating system patching is up to date
Recommended Control 01:	Agencies should develop a hardened SOE for workstations and servers, covering: x removal of unneeded software and operating system components x removal or disabling of unneeded services, ports and BIOS settings x disabling of unused or undesired functionality in software and operating systems x implementation of access controls on relevant objects to limit system users and programs to the minimum access required x installation of antivirus software x installation of software-based firewalls limiting inbound and outbound network connections x configuration of either remote logging or the transfer of local event logs to a central server x protection of audit and other logs through the use of a one-way pipe to reduce likelihood of compromise key transaction records
Recommended Control 02:	Agencies should ensure that for all servers and workstations: x virus detection heuristics are set to a high level x virus pattern signatures are checked for updates on at least a daily basis x virus pattern signatures are updated as soon as possible after vendors make them available

	x all disks and systems are regularly scanned for malicious code x the use of End Point Agents is considered
Recommended Control 03:	Agencies should reduce potential vulnerabilities in their SOEs by: x removing unused accounts x renaming or deleting default accounts x replacing default passwords, before or during the installation process
Recommended Control 04:	Where servers with a high security risk have connectivity to unsecure public networks, agencies should: x use appropriately rated gateways x consider the use of cross-domain solutions x segment networks x maintain effective functional segregation between servers allowing them to operate independently x minimize communications between servers at both the network and file system level as appropriate x limit system users and programs to the minimum access needed to perform their duties
Recommended Control 05:	Agencies should: x characterize all servers whose functions are critical to the agency, and those identified as being at a high security risk of compromise x store the characterization information securely off the server in a manner that maintains integrity x update the characterization information after every legitimate change to a system as part of the change control process x as part of the agency's ongoing audit schedule, compare the stored characterization information against current characterization information to determine whether a compromise, or a legitimate but incorrectly completed system modification, has occurred x perform the characterization from a trusted environment rather than the standard operating system wherever possible x resolve any detected changes in accordance with the agency's information security incident management procedures
Recommended Control 06:	Agencies should review all software applications to determine whether they attempt to establish any unauthorized or unplanned external connections

Recommended Control 07:	If automated outbound connection functionality is included, agencies should make a business decision to determine whether to permit or deny these connections, including an assessment of the security risks involved in doing so
Recommended Control 08:	If automated outbound connection functionality is included, Agencies should consider the implementation of Data Loss Prevention (DLP) technologies

The use of antivirus software, while adding value to the defense of workstations, cannot be relied solely upon to protect the workstation. As such agencies still need to deploy appropriately hardened SOEs to assist with the protection of workstations against a broader range of security risks.

Whilst a SOE can be sufficiently hardened when it is deployed, its security will progressively degrade over time. Agencies can address the degradation of the security of a SOE by ensuring that patches are continually applied, system users are not able to disable or bypass security functionality and antivirus and other security software is appropriately maintained with the latest signatures.

End Point Agents monitor traffic and apply security policies on applications, storage interfaces and data in real-time. Administrators actively block or monitor and log policy breaches. The End Point Agent can also create forensic monitoring to facilitate incident investigation. End Point Agents can also monitor user activity, such as the cut, copy, paste, print, print screen operations and copying data to external drives and other devices. The Agent can then apply policies to limit such activity.

Servers with a high security risk can include Web, email, file, Internet Protocol Telephony (IPT) servers and Mobile Device Manager (MDM) servers. It is important to clearly identify all services and connections to design a complete and secure server separation architecture.

There are known techniques for defeating basic characterizations, therefore other methods of intrusion detection are also needed, particularly in situations where it is impractical to use a trusted environment for the generation of the characterization data. Characterization is very useful in post-intrusion forensic investigations where an infected disk can be compared to stored characterization data in order to determine what files have been changed or introduced.

Characterization is also directly related to business continuity and disaster recovery and is influenced by Business Impact Analyses and Risk Assessments. Grouping elements by business applications and setting priority and criticality of the elements to the business may assist in determining the most appropriate and useful characterizations.

17.2. Application Whitelisting

Objective	Only approved applications are used on operating systems
Mandatory Control 01:	Agencies must ensure that a system user cannot disable the application whitelisting mechanism
Recommended Control 01:	Agencies should implement application whitelisting as part of the SOE for workstations, servers and any other network device
Recommended Control 02:	Agencies should prevent a system user from running arbitrary executables
Recommended Control 03:	Agencies should restrict a system user's rights in order to permit them to only execute a specific set of predefined executables as required for them to complete their duties
Recommended Control 04:	Agencies should ensure that application whitelisting does not replace the antivirus software within a system
Recommended Control 05:	Agencies should ensure that system administrators are not automatically exempt from application whitelisting policy
Recommended Control 06:	Agencies should ensure that the default policy is to deny the execution of software
Recommended Control 07:	Agencies should ensure that application whitelisting is used in addition to a strong access control list model and the use of limited privilege accounts
Recommended Control 08:	Agencies should plan and test application whitelisting mechanisms and processes thoroughly prior to implementation
Recommended Control 09:	Agencies should restrict the decision whether to run an executable based on the following, in the order of preference shown: x validates cryptographic hash x executable absolute path x digital signature x parent folder
Recommended Control 10:	Agencies should restrict the process creation permissions of any executables which are permitted to run by the application whitelisting controls
Recommended Control 11:	Logs from the application whitelisting implementation should include all relevant information

Application whitelisting can be an effective mechanism to prevent the successful compromise of an agency system resulting from the exploitation of a vulnerability in an application or the execution of malicious code. Defining a list of trusted executables, a whitelist, is a practical and secure method of securing a system rather than relying on a list of bad executables (black list) to be prevented from running. Application whitelisting is considered a part of a defense-in-depth strategy in order to prevent a successful attack, or to help mitigate consequences arising from an attack.

Further information on application whitelisting as implemented by Microsoft can be found at http://technet.microsoft.com/en-us/library/bb457006.aspx

An average system user requires access to only a few applications, or groups of applications, in order to conduct their work. Restricting the system user's permissions to execute code to this limited set of applications reduces the attack surface of the system. Since the consequences of running malicious code as a privileged user are much more severe than an unprivileged user, an application whitelisting implementation should also be enforced for system administrators.

17.3. Web Applications

Objective	**Access to Web content is implemented in a secure and accountable manner**
Mandatory Control 01:	Agencies must develop and implement a policy governing appropriate Web usage
Recommended Control 01:	Agencies should use a Web proxy for all Web browsing activities
Recommended Control 02:	An agency's Web proxy should authenticate system users and provide logging that includes at least the following details about websites accessed: x address (uniform resource locator) x time/date x system user x internal IP address x external IP address
Recommended Control 03:	Agencies should not permit downloading of executable files from external websites unless there is a demonstrable and approved business requirement
Recommended Control 04:	Agencies should disable the automatic launching of files downloaded from external websites
Recommended Control 05:	Agencies permitting SSL/TLS through their gateways should implement: x a solution that decrypts and inspects the SSL/TLS traffic as per content filtering requirements x a whitelist specifying the addresses (uniform resource locators) to which encrypted connections are permitted, with all other addresses blocked
Recommended Control 06:	Agencies should implement whitelisting for all HTTP traffic being communicated through their gateways
Recommended Control 07:	Agencies using a whitelist on their gateways to specify the external addresses, to which encrypted connections are permitted, should specify whitelist addresses by domain name or IP address

Recommended Control 08:	If agencies do not whitelist websites, they should blacklist websites to prevent access to known malicious websites
Recommended Control 09:	Agencies blacklisting websites should update the blacklist on a frequent basis to ensure that it remains effective
Recommended Control 10:	Agencies should block client-side active content, such as Java and ActiveX, which are assessed as having a limited business impact
Recommended Control 11:	Agencies should: x use client-side controls that allow JavaScript on a per website basis x add JavaScript functions used only for malicious purposes to the agency Web content filter or IDS/IPS
Recommended Control 12:	Agencies should use the Web proxy to filter content that is potentially harmful to system users and their workstations
Recommended Control 13:	Users should not store web site authentication credentials (user ID and password) on workstations, remote access devices (such as laptops) or BYO[8] devices
Recommended Control 14:	Users should not use the same password for multiple websites

Web proxies provide valuable information in determining if malicious code is performing regular interactions over Web traffic. Web proxies also provide usable information if system users are violating agency Web usage policies.

As SSL/TLS encrypted Web traffic travelling over HTTPS connections can deliver content without any filtering, agencies can reduce this security risk by using SSL/TLS inspection so that the Web traffic can be filtered. An alternative of using a whitelist for HTTPS websites can allow websites that have a low security risk of delivering malicious code and have a high privacy requirement like Web banking, to continue to have end-to-end encryption.

Defining a whitelist of permitted websites and blocking all unlisted websites limits one of the most common data delivery and exfiltration techniques used by malicious code. However, if agency personnel have a legitimate requirement to access a numerous and rapidly changing list of websites, agencies will need to consider the practicality and costs of such an implementation. In such cases black listing is a limited but none-the-less effective measure.

A Web whitelisting software application that allows for the management of whitelists can be obtained from http://whitetrash.sourceforge.net

Software that runs on agency systems should be controlled by the agency. Active content delivered though websites should be constrained so that it cannot arbitrarily access system users' files or

[8] Bring your own device

deliver malicious code. Unfortunately the implementations of Web browsers regularly contain flaws that permit such activity.

Examples of client-side JavaScript controls are available at http://noscript.net

Using a Web proxy provides agencies with an opportunity to filter potentially harmful information to system users and their workstations.

Some websites require the use of a user ID and password as the authentication mechanism. The management of passwords on these websites is often insecure and there are numerous examples of compromises where tens of thousands, and sometimes millions of passwords are compromised in a single incident. Where the same password is used on multiple websites, an incident can potentially compromise the user's account on À €Ç website using that password. It is important to treat these websites as insecure and manage passwords appropriately.

17.4. Software Application Development

Objective	**Secure programming methods and testing are used for application development in order to minimize the number of coding errors and security vulnerabilities**
Recommended Control 01:	Agencies should ensure that software development environments are configured such that: x there are at least three separate environments covering: ƒ development ƒ testing ƒ production x information flow between the environments is strictly limited according to a defined and documented policy, with access granted only to system users with a clear business requirement x new development and modifications only take place in the development environment x write access to the authoritative source for the software (source libraries & production environment) is disabled
Recommended Control 02:	Agencies should ensure that software developers use secure programming practices when writing code, including: x designing software to use the lowest privilege level needed to achieve its task x denying access by default x checking return values of all system calls x validating all inputs
Recommended Control 03:	Software should be reviewed or tested for vulnerabilities before it

	is used in a production environment
Recommended Control 04:	Software should be reviewed or tested by an independent party as well as the developer
Recommended Control 05:	Software development should follow secure coding practices and agency development standards

Software development should follow recognized good practice, segregates development, testing and production environments to limit the spread of malicious code and minimize the likelihood of faulty code being put into production. Limiting access to development and testing environments will reduce the information that can be gained by an internal attacker.

Designing software should use the lowest privilege level needed to achieve its task will limit the privileges an attacker could gain in the event they subvert the software security. Validating all inputs will ensure that the input is within expected ranges, reducing the chance that malicious or erroneous input causes unexpected results.

Software reviewing and testing will reduce the possibility of introducing vulnerabilities into a production environment. Using an independent party for software testing will limit any bias that can occur when a developer tests their own software.

17.5. Web Application Development

Objective	**Security mechanisms are incorporated into all Web applications by design and implementation**
Recommended Control 01:	Agencies should review all active content on their Web servers for known information security issues
Recommended Control 02:	Agencies should minimize connectivity and access between each Web application component
Recommended Control 03:	Agencies should follow the documentation provided in the Open Web Application Security Project guide to building secure Web applications and Web services

Even though Web servers may contain only information authorized for release into the public domain, there still remains a need to protect the integrity and availability of the information. As such, Web servers are to be treated in accordance with the requirements of the classification of the system they are connected to. Web application components at a high level consist of a Web server for presentation, a Web application for processing and a database for content storage. There can be

more or fewer components, however in general there is a presentation layer, application layer and database layer.

Reviewing active content on agency Web servers will assist in identifying and mitigating information security issues.

Web applications are typically very exposed services that provide complex interactions with system users. This greatly increases the security risk of being compromised. By segregating components the impact of potential application flaws or attacks is limited.

The Open Web Application Security Project guide provides a comprehensive resource to consult when developing Web applications.

18. Email Security

18.1. Email Applications

Objective	Email messages have appropriate protective markings to facilitate the application of handling instructions
Mandatory Control 01:	Agencies must develop and implement a policy governing the use of email
Mandatory Control 02:	Agencies must make their system users aware of the agency's email usage policies
Recommended Control 01:	Personnel should not send emails that contain active Web addresses or click on active Web addresses within emails they receive
Recommended Control 02:	Agencies should implement measures to monitor their personnel's compliance with email usage policies
Recommended Control 03:	Agencies should not allow personnel to use public Web-based email services, for processing, receiving or sending emails or attachments for official business

There are many security risks associated with the unsecure nature of email that are often overlooked. Documenting them will inform information owners about these security risks and how they might affect business operations.

Spoofed emails often contain an active Web address directing personnel to a malicious website to either elicit information or infect their workstation with malicious code. In order to reduce the success rate of such attacks agencies can choose to educate their personnel to neither send emails with active Web addresses or to click on Web addresses in emails that they receive.

Using public Web-based email services may allow personnel to bypass security measures that agencies will have put in place to protect against malicious code or phishing attempts distributed via email. Web based email services may also by-pass agency context filtering mechanisms.

18.2. Email Infrastructure

Objective	Email infrastructure is hardened and email is secured
Mandatory Control 01:	Where an agency has system users that send email from outside the agency's network, an authenticated and encrypted channel must be configured to allow email to be sent via the centralised

Objective	Email infrastructure is hardened and email is secured
	email gateway
Mandatory Control 02:	Agencies must enable opportunistic TLS encryption as defined in IETF's RFC 3207[9] on email servers that make incoming or outgoing email connections over public infrastructure
Mandatory Control 03:	Agencies must: x specify mail servers using SPF or Sender ID x mark, block or identify incoming emails that fail SPF checks for notification to the email recipient
Recommended Control 01:	Agencies should configure the following gateway filters: x inbound and outbound email, including any attachments, that contain: ƒ malicious code ƒ content in conflict with the agency's email policy ƒ content that cannot be identified ƒ blacklisted or unauthorized file types x encrypted content, when that content cannot be inspected for malicious code or authenticated as originating from a trusted source x emails addressed to internal email aliases with source addresses located from outside the domain x all emails arriving via an external connection where the source address uses an internal agency domain
Recommended Control 02:	Email servers should be configured to strip active addresses and URL's and replace them with text only versions
Recommended Control 03:	Agencies should configure systems to log every occurrence of a blocked email
Recommended Control 04:	Agencies should send notification of undeliverable, bounced or blocked emails to senders that can be verified via SPF or other trusted means
Recommended Control 05:	Agencies should disable open email relaying so that email servers will only relay messages destined for the agency's domain(s) and those originating from within that domain
Recommended Control 06:	Agencies should perform regular email server auditing, security reviews and vulnerability analysis activities
Recommended Control 07:	Agencies should route email through a centralized email gateway
Recommended Control 08:	Where backup or alternative email gateways are in place, additional email gateways should be maintained at the same standard as the primary email gateway
Recommended Control 09:	Agencies should:

[9](RFC3207, 2002)

Objective	Email infrastructure is hardened and email is secured
	x use a hard fail SPF record when specifying email servers x use SPF[10] or Sender ID to verify the authenticity of incoming emails
Recommended Control 10:	Agencies should refer to the SPF recommendations in IETF's RFC 7208[11]
Recommended Control 11:	Agencies should enable DKIM[12] signing on all email originating from their domain
Recommended Control 12:	Agencies should use DKIM in conjunction with SPF
Recommended Control 13:	Agencies should verify DKIM signatures on emails received, taking into account that email distribution list software typically invalidates DKIM signatures
Recommended Control 14:	Where agencies operate email distribution list software used by external senders, agencies should configure the software so that it does not impair the validity of the sender's DKIM signature

The intent of blocking specific types of emails is to reduce the likelihood of phishing emails and emails or attachments containing malicious code entering the agency's networks.

Spoofed emails often contain an active (embedded) email address directing users to a malicious website in order to infect the workstation or agency systems with malicious code. An effective defense is to strip and replace active addresses and hyperlinks with text only versions.

Undeliverable or "bounce" emails are commonly sent by email servers to the original sender when the email cannot be delivered, often because the destination address is invalid. Because of the common spamming practice of spoofing sender addresses, this can result in a large amount of bounce emails being sent to an innocent third party. Sending bounces only to senders that can be verified via the Sender Policy Framework (SPF) or other trusted means avoids contributing to this problem and allows other government agencies and trusted parties to receive legitimate bounce messages.

An open relay email server (or open mail relay) is a server that is configured to allow anyone on the Internet to send emails through the server. Such configurations are highly undesirable as they allow spammers and worms to exploit this functionality to send emails through the server.

Without a centralized email gateway it is exceptionally difficult to deploy Sender Policy Framework (SPF). Attackers will almost invariably avoid using the primary email server when sending malicious

[10]Sender Policy Framework (SPF) is a simple email-validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators.
[11](RFC7208, 2014)
[12] Domain Keys Identified Mail (DKIM) allows senders to associate a domain name with an email message, thus vouching for its authenticity. This is done by "signing" the email with a digital signature, a field that is added to the message's header.

emails. This is because the backup or alternative gateways are often poorly maintained with out-of-date blacklists and content filtering.

Email can be intercepted anywhere between the originating email server and the destination email server. Email transport between organizations and agencies is usually over the internet or other unsecured public infrastructure so it is important that email interception is carefully managed and suitable controls applied. One effective measure is to use TLS to encrypt the email traffic **between email servers**. Enabling TLS on the originating and accepting email server will defeat passive attacks on the network, with the exception of cryptanalysis against email traffic. TLS encryption **between email servers** will not interfere with email content filtering schemes. Email servers will remain compatible with other email servers as IETF's RFC 3207 specifies the encryption as opportunistic.

The Sender Policy Framework (SPF) is an open standard specifying a technical method to prevent sender address forgery. An SPF-protected domain is less attractive to spammers and phishers because the forged e-mails are more likely to be caught in spam filters which check the SPF record. Because an SPF-protected domain is less attractive as a spoofed address, it is less likely to be blacklisted by spam filters and so is less disruptive to email traffic. Having a proper Sender Policy Framework (SPF) record increases the chances people will get emails you send. Without one, your email has a greater chance of being marked as Spam. SPF and alternatives such as Sender ID aid in the detection of spoofed email server address domains. The SPF record specifies a list of IP addresses or domains that are allowed to send mail from a specific domain. If the email server that transmitted the email is not in the list, the verification fails (there are a number of different fail types available).

DKIM enables a method of determining spoofed email content. The DKIM record specifies a public key that will sign the content of the message. If the signed digest in the email header doesn't match the signed content of the email the verification fails.

19. Access Control

19.1. Identification and Authentication

Objective	Identification and authentication requirements are implemented in order to provide a secure means of access to information and systems
Mandatory Control 01:	Agencies must: x develop and maintain a set of policies and procedures covering system users': x identification x authentication x authorisation x make their system users aware of the agency's policies and procedures
Mandatory Control 02:	Agencies must ensure that all system users are: x uniquely identifiable x authenticated on each occasion that access is granted to a system
Mandatory Control 03:	If agencies choose to allow shared, non-user-specific accounts they must ensure that an independent means of determining the identification of the system user is implemented
Mandatory Control 04:	Agencies must not use a numerical password (or personal identification number) as the sole method of authenticating a system user to access a system
Mandatory Control 05:	Agencies must not allow storage of unprotected authentication information that grants system access, or decrypts an encrypted device, to be located on, or with the system or device, to which the authentication information grants access
Mandatory Control 06:	Agencies must ensure system users provide sufficient evidence to verify their identity when requesting a password reset for their system account
Recommended Control 01:	Agencies should not use shared credentials to access accounts
Recommended Control 02:	Agencies should ensure that they combine the use of multiple methods when identifying and authenticating system users
Recommended Control 03:	Agencies should implement a password policy enforcing either: x a minimum password length of 16 characters with no complexity requirement or x a minimum password length of ten characters, consisting of at least three of the following character sets:

	ƒ lowercase characters (a-z) ƒ uppercase characters (A-Z) ƒ digits (0-9) ƒ punctuation and special characters
Recommended Control 04:	Agencies should: x ensure that passwords are changed at least every 90 days x prevent system users from changing their password more than once a day x check passwords for compliance with their password selection policy where the system cannot be configured to enforce complexity requirements x force the system user to change an expired password on initial logon or if the password is reset
Recommended Control 05:	Agencies should not: x allow predictable reset passwords x reuse passwords when resetting multiple accounts x store passwords in the clear on the system x allow passwords to be reused within eight password changes x allow system users to use sequential passwords
Recommended Control 06:	Agencies should disable LAN[13] Manager for password authentication on workstations and servers
Recommended Control 07:	Agencies should develop and implement a policy to automatically logout and shutdown workstations after an appropriate time of inactivity
Recommended Control 08:	Agencies should: x configure systems with a session or screen lock x configure the lock to activate: ƒ after a maximum of 15 minutes of system user inactivity or ƒ if manually activated by the system user x configure the lock to completely conceal all information on the screen x ensure that the screen is not turned off or enters a power saving state before the screen or session lock is activated x have the system user re-authenticate to unlock the system x deny system users the ability to disable the locking mechanism

[13] Local Area Network

Recommended Control 09:	Agencies should: x lock system user accounts after three failed logon attempts x have a system administrator reset locked accounts x remove or suspend system user accounts as soon as possible when personnel no longer need access due to changing roles or leaving the agency x remove or suspend inactive accounts after a specified number of days
Recommended Control 10:	Agencies should have a logon banner that requires a system user to acknowledge and accept their security responsibilities before access to the system is granted
Recommended Control 11:	Agency logon banners should cover issues such as: x the system's description x access only being permitted to authorized system users x the system user's agreement to abide by relevant security policies x the system user's awareness of the possibility that system usage is being monitored x the definition of acceptable use for the system x legal ramifications of violating the relevant policies
Recommended Control 12:	Agencies should configure systems to display the date and time of the system user's previous login during the login process

Developing policies and procedures will ensure consistency in identification, authentication and authorization, across agency systems and with relevant standards.

Sharing passwords and UserIDs (credentials) may be convenient but invariably hampers efforts to identify a specific user and attribute actions to a specific person or system. While agencies and users find convenience in sharing credentials, doing so is highly risky. Shared credentials can defeat accountability and the attribution and non-repudiation principles of access control. This is particularly important where administrative access to networks and servers is provided through shared credentials.

However, agencies may have a compelling business reason for the use of shared accounts. These may include Anonymous, Guest and Temporary Employee (such relieving a receptionist) credentials. It may not be possible to attribute the use of such accounts to a specific person. As shared accounts are non-user-specific, agencies will need to determine an appropriate method of attributing actions undertaken by such accounts to specific personnel. For example, a logbook may be used to document the date and time that a person takes responsibility for using a shared account and the actions logged against the account by the system.

Limiting the storage of unprotected authentication information reduces the possibility of an attacker finding and using the information to access a system under the guise of a valid system user.

Passwords are the primary authentication mechanism for almost all information systems and are fundamental part of access and authentication processes and mechanisms. While there are some limitations in the use of passwords, they remain the most cost effective means available with current technology.

Password controls are designed to manage known risks and attack methods using the controls specified in this section. For example, passwords with at least ten characters utilizing upper and lower case, numbers and special characters have a much greater resistance to brute force attacks. When use in combination with controls such as password history and regular password change, passwords can present high resistance to known attack methods.

A logon banner for a system serves to remind system users of their responsibilities when using the system. It may also be described as a “Splash Screen” or “User Consent Screen”.

Displaying when a system user has last logged onto a system will assist system users in identifying any unauthorized use of their account. Accordingly, when any case of unauthorized use of an account is identified, it should be reported to an ITSM immediately for investigation.

19.2. System Access

Objective	**Access to information on systems is controlled in accordance with agency policy and this manual**
Mandatory Control 01:	Agencies must have authorisation of system users enforced by access controls
Mandatory Control 02:	Agencies must restrict access to compartmented information. Such restriction must be enforced by the system

19.3. Privileged Access

Objective	**Only trusted personnel are granted privileged access to systems**
Recommended Control 01:	Agencies should: x ensure strong change management practices are implemented x ensure that the use of privileged accounts is controlled and accountable

	x ensure that system administrators are assigned an individual account for the performance of their administration tasks x keep privileged accounts to a minimum x allow the use of privileged accounts for administrative work only

Inappropriate use of any feature or facility of a system that enables a privileged user to override system or application controls can be a major contributory factor to failures, information security incidents, or system breaches. Privileged access rights allow for system wide changes to be made and as such an appropriate and effective mechanism to log privileged users and strong change management practices will provide greater accountability and auditing capability.

19.4. Remote Access

Objective	**Remote access to systems is minimized, secure, controlled, authorized and authenticated**
Mandatory Control 01:	Agencies must authenticate each remote connection and user prior to permitting access to an agency system
Recommended Control 01:	Agencies should authenticate both the remote system user and device during the authentication process
Recommended Control 02:	Agencies should not allow the use of remote privileged access from an untrusted domain, including logging in as an unprivileged system user and then escalating privileges
Recommended Control 03:	Agencies should establish VPN connections for all remote access connections

Remote access is defined as user access to agency systems originating outside an agency network. The requirements for using multi–factor authentication are described in the Identification and Authentication section of this chapter.

Remote access by a privileged user to an agency system via a less trusted security domain (for example, the Internet) may present additional risks. Controls in this section are designed to prevent escalation of user privileges from a compromised remote access account.

19.5. Event Logging and Auditing

Objective	**Information security related events are logged and audited for accountability, incident management, forensic and system monitoring purposes**

Mandatory Control 01:	Agencies must develop and document logging requirements covering: x the logging facility, including: ƒ log server availability requirements ƒ the reliable delivery of log information to the log server x the list of events associated with a system or software component to be logged x event log protection and archival requirements
Mandatory Control 02:	For each event identified as needing to be logged, agencies must ensure that the log facility records at least the following details, where applicable: x date and time of the event x relevant system user(s) or processes x event description x success or failure of the event x event source (e.g. application name) x IT equipment location/identification
Mandatory Control 03:	Event logs must be protected from: x modification and unauthorised access x whole or partial loss within the defined retention period
Mandatory Control 04:	Event logs must be archived and retained for an appropriate period as determined by the agency
Mandatory Control 05:	Disposal or archiving of DNS[14], proxy[15], event, systems and other operational logs must be in accordance with the provisions or the relevant legislation
Mandatory Control 06:	Agencies must develop and document event log audit requirements covering: x the scope of audits x the audit schedule x action to be taken when violations are detected x reporting requirements x roles and specific responsibilities
Recommended Control 01:	Agencies should determine a policy for the retention of system management logs
Recommended Control 02:	A system management log should record the following minimum information: x all system start-up and shutdown

[14] The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses.

[15] A proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.

	x service, application, component or system failures x maintenance activities x backup and archival activities x system recovery activities x special or out of hours' activities
Recommended Control 03:	Agencies should log the events listed in the Annex 6 for specific software components
Recommended Control 04:	Agencies should log, at minimum, the following events for all software components: x user login x all privileged operations x failed attempts to elevate privileges x security related system alerts and failures x system user and group additions, deletions and modification to permissions x unauthorized or failed access attempts to systems and files identified as critical to the agency
Recommended Control 05:	Agencies should establish an authoritative time source
Recommended Control 06:	Agencies should synchronize all logging and audit trails with the time source to allow accurate time stamping of events
Recommended Control 07:	Agencies should ensure that: x systems are configured to save event logs to a separate secure log server x event log data is archived in a manner that maintains its integrity
Recommended Control 08:	Agencies should retain DNS, proxy and event logs for at least 18 months

A security event is a change to normal or expected behavior of a network, network component, system, device or user. Event logging helps improve the security posture of a system by increasing the accountability of all user actions, thereby improving the chances that malicious behavior will be detected.

It is important that sufficient details are recorded in order for the logs to be useful when reviewed or when an investigation is in progress. Retention periods are also important to ensure sufficient log history is available. Conducting audits of event logs is an integral part of the security and maintenance of systems, since they will help detect and attribute any violations of information security policy, including cyber security incidents, breaches and intrusions.

20. Cryptography

20.1. Cryptographic Fundamentals

Objective	Cryptographic implementations by agencies are adequate for the protection of data and communications
Recommended Control 01:	Cryptographic products should provide a means of data recovery to allow for recovery of data in circumstances where the encryption key is unavailable due to loss, damage or failure
Recommended Control 02:	Agencies should use a secure encryption product if they wish to communicate over insecure or unprotected networks such as the Internet

It is important for continuity and operational stability that cryptographic products provide a means of data recovery to allow for the recovery of data in circumstances such as where the encryption key is unavailable due to loss, damage or failure. This includes production, storage, backup and virtual systems.

20.2. Secure Sockets Layer and Transport Layer Security

Objective	Information in transit is protected by an Approved Cryptographic Protocol implementing an Approved Cryptographic Algorithm
Recommended Control 01:	Agencies should use the current version of TLS[16]
Recommended Control 02:	Agencies shouldnot use any version of SSL[17]

Secure Sockets Layer (**SSL**), and **Transport Layer Security** (**TLS**) are cryptographic protocols designed to provide communication security when using the Internet. They use X.509 certificates and asymmetric cryptography for authentication purposes. This generates a session key. This session key is then used to encrypt data between the parties. Encryption with the session key provides data and message confidentiality, and message authentication codes for message integrity.

However, a number of vulnerabilities has been found in SSL, thus SSL should be replaced by TLS.

7UDQVSRUW /D\HU 6HFXULW\
6HFXUH 6RFNHWV /D\HU

20.3. Secure Shell

Objective	Secure Shell (SSH) is implemented correctly as an Approved Cryptographic Protocol
Recommended Control 01:	Settings that should be implemented when using SSH: **Configuration description** — **Configuration directive** Disallow the use of SSH version 1 — Protocol 2 On machines with multiple interfaces, configure the SSH daemon to listen only on the required interfaces — ListenAddressxxx.xxx.xxx.xxx Disable connection forwarding — AllowTCPForwarding no Disable gateway ports — Gatewayports no Disable the ability to login directly as root — PermitRootLogin no Disable host-based authentication — HostbasedAuthentication no Disable rhosts-based authentication — RhostsAuthentication no IgnoreRhosts yes Do not allow empty passwords — PermitEmptyPasswords no Configure a suitable login banner — Banner/directory/filename Configure a login authentication timeout of no more than 60 seconds — LoginGraceTime xx Disable X forwarding — X11Forwarding no
Recommended Control 02:	Agencies should use public key-based authentication before using password-based authentication
Recommended Control 03:	Agencies that allow password authentication should use techniques to block brute force[18] attacks against the password
Recommended Control 04:	Agencies should use parameter checking when using the 'forced command' option
Recommended Control 05:	Agencies that use logins without a password for automated purposes should disable: x access from IP addresses that do not need access x port forwarding x agent credential forwarding x X11 display remoting x console access

[18] A brute-force attack, or exhaustive key search, is a cryptanalytic attack that can, in theory, be used against any encrypted data (except for data encrypted in an information-theoretically secure manner)

Recommended Control 06:	Agencies that use remote access without the use of a password should use the 'forced command' option to specify what command is executed
Recommended Control 07:	Agencies that use SSH-agent or other similar key caching programs should: x only use the software on workstation and servers with screen locks x ensure that the key cache expires within four hours of inactivity x ensure that agent credential forwarding is used when multiple SSH transversal is needed
Recommended Control 08:	Ensure that the latest implementation of SSH software is being used. Older versions contain known vulnerabilities

SSH is software based on the Secure Shell protocol and enables a connection to a remote system

SSH version 1 is known to have vulnerabilities. In particular, it is susceptible to a man-in-the-middle attack, where an attacker who can intercept the protocol in each direction can make each node believe they are talking to the other. SSH version 2 does not have this vulnerability.

Public key-based systems have greater potential for strong authentication, put simply people are not able to remember particularly strong passwords. Password-based authentication schemes are also more susceptible to interception than public key-based authentication schemes. Passwords are more susceptible to guessing attacks, so if passwords are used in a system then countermeasures should be put into place to reduce the chance of a successful brute force attack.

If password-less authentication is enabled, allowing access from unknown IP addresses would allow untrusted parties to automatically authenticate to systems without needing to know the password
If port forwarding is not disabled or it is not configured securely, an attacker may be able to gain access to forwarded ports and thereby create a communication channel between the attacker and the host. If agent credential forwarding is enabled, an intruder could connect to the stored authentication credentials and then use them to connect to other trusted hosts or even intranet hosts, if port forwarding has been allowed as well.

X11 is a computer software system and network protocol that provides a graphical user interface for networked computers. Failing to disable X11 display remoting could result in an attacker being able to gain control of the computer displays as well as keyboard and mouse control functions.

Allowing console access allows every user who logs into the console to run programs that are normally restricted to the root user.

SSH-agent or other similar key caching programs hold and manage private keys stored on workstations and respond to requests from remote systems to verify these keys. When an SSH-

agent launches, it will request the user's password. This password is used to unlock the user's private key. Subsequent access to remote systems is performed by the agent and does not require the user to re-enter their password. Screen locks and expiring key caches ensure that the user's private key is not left unlocked for long periods of time. Agent credential forwarding is required when multiple SSH connections are chained to allow each system in the chain to authenticate the user.

20.4. Secure Multipurpose Internet Mail Extension

Objective	**Secure Multipurpose Internal Mail Extension (S/MIME) is implemented correctly as an approved cryptographic protocol**
Mandatory Control 01:	Decommissioning of faulty or equipment to be replaced must comply with media sanitisation requirements described in Chapter 15 - Product Security
Mandatory Control 02:	Agencies mustassure that the latest implementation of S/MIME is used

Version 3.0 of S/MIME is the first version to become an Internet Engineering Taskforce (IETF) standard.

Agencies choosing to implement S/MIME should be aware of the inability of many content filters to inspect encrypted messages and any attachments for inappropriate content, and for server-based antivirus software to scan for viruses and other malicious code.

Improper decommissioning and sanitization presents opportunities for harvesting Private Keys. Products that hosted multiple Private Keys for the management of multiple identities should be considered points of aggregation with an increased "target value". Where cloud based computing services have been employed, media sanitization may be problematic and require the revocation and re-issue of new keys.

20.5. Open PGP Message Format

Objective	**Open PGP Message Format is implemented correctly as an Approved Cryptographic Protocol**
Mandatory Control 01:	Agencies must immediately revoke key pairs when a private certificate is suspected of being compromised or leaves the control of the agency

If the private certificate and associated key used for encrypting messages is suspected of being compromised i.e. stolen, lost or transmitted over the Internet, then no assurance can be placed in

the integrity of subsequent messages that are signed by that private key. Likewise no assurance can be placed in the confidentiality of a message encrypted using the public key as third parties could intercept the message and decrypt it using the private key.

20.6. Internet Protocol Security

Objective	Internet Protocol Security (IPSec) is correctly implemented
Recommended Control 01:	Agencies should use tunnel mode for IPSec connections
Recommended Control 02:	Agencies choosing to use transport mode should additionally use an IP tunnel for IPSec connections
Recommended Control 03:	Agencies should use the ESP[19] protocol for IPSec connections
Recommended Control 04:	Agencies using ISAKMP[20]should disable aggressive mode for IKE
Recommended Control 05:	Agencies should use a security association lifetime of four hours or 14400 seconds, or less
Recommended Control 06:	Agencies should use HMAC-SHA256[21], HMAC-SHA384[22] or HMAC-SHA512[23] as the HMAC algorithm
Recommended Control 07:	Agencies should use the largest modulus size available for the DH exchange
Recommended Control 08:	Agencies should use Perfect Forward Secrecy for IPSec connections
Recommended Control 09:	Agencies should disable the use of XAUTH[24] for IPSec connections using IKEv1[25]

IPSec can be operated in two modes: transport mode or tunnel mode. The tunnel mode of operation provides full encapsulation of IP packets whilst the transport mode of operation only encapsulates the payload of the IP packet.

Most IPSec implementations can handle a number of cryptographic algorithms for encrypting data when the ESP protocol is used. These include 3DES and AES. Most IPSec implementations handle a number of methods for sharing keying material used in hashing and encryption processes. Two common methods are manual keying and IKE using the ISAKMP. Both methods are considered suitable for use.

[19] Encapsulating Security Payload
[20] Internet Security Association and Key Management Protocol
[21](HMAC-SHA256)
[22](HMAC-SHA384)
[23](HMAC-SHA512)
[24]XAuth is a second-factor authentication plugin that can be used to secure player accounts on server.
[25] Internet Key Exchange

Most IPSec implementations handle a number of methods for authentication as part of ISAKMP. These can include digital certificates, encrypted nonce or pre-shared keys. All these methods are considered suitable for use.

In order to provide a secure VPN style connection both authentication and encryption are needed. ESP is the only way of providing encryption yet AH and ESP can provide authentication for the entire IP packet and the payload respectively. ESP is generally preferred for authentication though as AH has inherent network address translation limitations.

ISAKMP uses two modes to exchange information as part of IKE. These are main mode and aggressive mode. Using main mode instead of aggressive mode provides greater security since all exchanges are protected.

Using a secure association lifetime of four hours or 14400 seconds provides a balance between security and usability.

XAUTH using IKEv1 has documented vulnerabilities associated with its use.

20.7. Key Management

Objective	**Cryptographic keying material is protected by key management procedures**
Mandatory Control 01:	Before personnel are granted cryptographic system administrator access, agencies must ensure that they have: x a demonstrated need for access x read and agreed to comply with the relevant KMP for the cryptographic system they are using x a security clearance at least equal to the highest classification of the cryptographic system x agreed to protect the authentication information for the cryptographic system at the highest classification of information it secures x agreed not to share authentication information for the cryptographic system without approval x agreed to be responsible for all actions under their accounts x agreed to report all potentially security related problems to the BCC x ensure relevant staff have received appropriate training
Mandatory Control 02:	Agencies must conduct audits using two personnel with cryptographic system administrator access

Objective	Cryptographic keying material is protected by key management procedures
Mandatory Control 03:	Agencies must hold and maintain an access register that records cryptographic system information such as: x details of personnel with system administrator access x details of those whose system administrator access was withdrawn x details of system documents x accounting activities x audit activities
Recommended Control 01:	Agencies should be able to readily account for all transactions relating to cryptographic system material including identifying hardware and all software versions issued with the equipment and materials, including date and place of issue
Recommended Control 02:	Agencies should conduct audits of cryptographic system material: x on handover/takeover of administrative responsibility for the cryptographic system x on change of personnel with access to the cryptographic system x at least annually
Recommended Control 03:	Agencies should perform audits to: x account for all cryptographic system material x confirm that agreed security measures documented in the KMP[26] are being followed
Recommended Control 04:	Cryptographic system equipment should be stored in a room that meets the requirements for a server room
Recommended Control 05:	Areas in which cryptographic system material is used should be separated from other areas and designated as a controlled cryptography area
Recommended Control 06:	Agencies should develop a KMP when they have implemented a cryptographic system using commercial grade cryptographic equipment
Recommended Control 07:	The minimum contents which should be documented in the KMP are: x Accounting – how accounting will be undertaken for the cryptographic system, what records will be maintained and how records will be audited x Classification – what is the classification of cryptographic system hardware, software and documentation

[26] .QXWK 0RUULV 3UDWW DOJRULWKP

Objective	Cryptographic keying material is protected by key management procedures
	❍ Information security incidents – a description of the conditions under which compromise of key material should be declared and references to procedures to be followed when reporting and dealing with information security incidents X Key management – who generates keys, how keys are delivered and received, key distribution (local, remote, central), how keys are installed, transferred, stored, recovered, revoked and destroyed X Roles – documenting roles of COMSEC Custodian, record keeper and auditor X Maintenance – maintaining the cryptographic system hardware and software and destroying equipment and media X Objectives – objectives of the cryptographic system and KMP, including organizational aims X System description – maximum classification of information protected, the use of keys, the environment, administrative responsibilities, key algorithm, length and lifetime. X Topology – diagram(s) and description of the cryptographic system topology including data flows

The cryptographic system administrator is a highly privileged position which involves granting privileged access to a cryptographic system. Therefore extra precautions need to be put in place surrounding the security and vetting of the personnel as well as the access control procedures for individuals designated as cryptographic system administrators.

As cryptographic equipment, and the keys they store, provide a significant security function for systems it is important that agencies are able to account for all cryptographic equipment. Cryptographic system audits are used as a process to account for cryptographic equipment.

As cryptographic equipment contains particularly sensitive information additional physical security measures need to be applied to the equipment.

Access registers can assist in documenting personnel that have privileged access to cryptographic systems along with previous accounting and audit activities for the system.

21. Network Security

21.1. Network Management

Objective	Any change to the configuration of networks is authorized and controlled through appropriate change management processes to ensure security, functionality and capability is maintained
Mandatory Control 01:	Agencies must perform a security risk assessment before providing network documentation to a third party, such as a commercial provider or contractor
Mandatory Control 02:	Network documentation provided to a third party, such as to a commercial provider or contractor, must contain only the information necessary for them to undertake their contractual services and functions, in line with the need-to-know principle
Mandatory Control 03:	Detailed network configuration information must not be published in tender documentation
Mandatory Control 04:	For each network an agency manages they must have: x a high-level diagram showing all connections and gateways into the network x a network diagram showing all communications equipment
Recommended Control 01:	Security aspects should be considered when determining the classification level of systems and network documentation
Recommended Control 02:	Agencies should keep the network configuration under the control of a network management authority
Recommended Control 03:	All changes to the configuration should be documented and approved through a formal change control process
Recommended Control 04:	Agencies should regularly review their network configuration to ensure that it conforms to the documented network configuration
Recommended Control 05:	Agencies should deploy an automated tool that compares the running configuration of network devices against the documented configuration
Recommended Control 06:	An agency's network diagrams should: x be updated as network changes are made x include a 'Current as at [date]' statement on each page
Recommended Control 07:	Agencies should implement network access controls on all networks
Recommended Control 08:	Agencies should implement protection measures to minimize the risk of unauthorized access to network management traffic on a

Objective	Any change to the configuration of networks is authorized and controlled through appropriate change management processes to ensure security, functionality and capability is maintained
	network

An agency's network diagrams should illustrate all network devices including firewalls, IDSs, IPSs, routers, switches, hubs, etc. It does not need to illustrate all IT equipment on the network, such as workstations or printers which can be collectively represented. The inclusion of significant devices such as MFD's and servers can aid interpretation.

To provide an appropriate level of protection to systems and network documentation, a number of security aspects should be considered. These will include the existence of the system, the intended use, the connectivity and agencies connected, protection enhancements and modifications and the level of detail included in the documentation. High level conceptual diagrams and accompanying documentation should also be subject to these considerations.

If the network is not centrally managed, there could be sections of the network that do not comply with the agency's security policies, and thus create a vulnerability. Changes should be authorized by a change management process, including representatives from all parties involved in the management of the network. This process ensures that changes are understood by all parties and reduces the likelihood of an unexpected impact on the network.

As most decisions are made on the documentation that illustrates the network, it is important that:

- a network diagram exists
- the security architecture is recorded
- the network diagram is an accurate depiction of the network and the network diagram indicates when it was last updated

If an attacker has limited opportunities to connect to a given network, they have limited opportunities to attack that network. Network access controls not only prevent against attackers traversing a network but also prevent system users carelessly connecting a network to another network. It is also useful in segregating sensitive or compartmented information for specific system users with a need-to-know.

The Simple Network Management Protocol (SNMP) can be used to monitor the status of network devices such as switches, routers and wireless access points. However, SNMP is considered insecure.

21.2. Wireless Local Area Networks

Objective	Wireless local area networks are deployed in a secure manner that does not compromise the security of information and systems
Mandatory Control 01:	Devices must not be configured to remember and automatically connect to any wireless networks that they have previously connected to
Mandatory Control 02:	Agencies deploying a wireless network for public access must segregate it from any other agency network
Mandatory Control 03:	All wireless access points used for government wireless networks must be Wi-Fi Alliance certified
Mandatory Control 04:	WPA2-Enterprise with EAP-TLS, WPA2-Enterprise with PEAP-EAP-TLS, WPA2-Enterprise with EAP-TTLS or WPA2-Enterprise with PEAP must be used on wireless networks to perform mutual authentication
Mandatory Control 05:	The certificates for both a device and user accessing a wireless network mustnot be stored on the same device
Mandatory Control 06:	Devices must be configured to validate the server certificate, disable any trust for certificates generated by commercial certificate authorities that are not trusted and disable the ability to prompt users to authorise new servers or commercial certification authorities
Mandatory Control 07:	Devices should be set to enable identity privacy
Mandatory Control 08:	TKIP and WEP support must be disabled or removed from wireless access points
Mandatory Control 09:	Agencies mustnot use WEP for wireless deployments
Mandatory Control 10:	Agencies must change the default SSID of wireless access points
Mandatory Control 11:	Agencies must rename or remove default accounts and passwords
Mandatory Control 12:	Where BYOD has been approved by an agency, any wireless network allowing BYOD connections must be segregated from all other agency networks, including any agency wireless networks
Mandatory Control 13:	Agencies mustnot allow non-agency devices to connect to agency controlled wireless networks not intended or configured for BYOD devices or for public access
Recommended Control 01:	Wireless auto-connect functionality on devices should be disabled, preferably by a hardware switch, whenever connected to a fixed network
Recommended Control 02:	Certificates stored on devices accessing wireless networks should be protected by implementing full disk encryption on the devices
Recommended Control 03:	Devices should be set to enable identity privacy

Objective	Wireless local area networks are deployed in a secure manner that does not compromise the security of information and systems
Recommended Control 04:	The PMK caching period shouldnot be set to greater than 1440 minutes (24 hours)
Recommended Control 05:	If pre-shared keys are used, agencies should use random keys of the maximum allowable length
Recommended Control 06:	Agencies shouldnot use pre-shared keys for wireless authentication
Recommended Control 07:	Agencies should disable the administrative interface on wireless access points for wireless connections
Recommended Control 08:	Wireless access points and devices should be upgraded to support a minimum of the 802.11w amendment
Recommended Control 09:	The SSID of a wireless network shouldnot be readily associated with an agency, the premises, location or the functionality of the network
Recommended Control 10:	Agencies shouldnot disable SSID broadcasting on wireless networks
Recommended Control 11:	Agencies should use the Dynamic Host Configuration Protocol (DHCP) for assigning IP addresses on wireless networks
Recommended Control 12:	MAC address filtering shouldnot be used as a security mechanism to restrict which devices connect to a wireless network
Recommended Control 13:	Key generation, distribution and rekeying procedures should be documented in the SecPlan for the wireless network
Recommended Control 14:	Wireless device drivers and their versions should be documented in the SecPlan for the wireless network
Recommended Control 15:	Agencies shouldnot allow agency devices to connect to non-agency controlled wireless networks
Recommended Control 16:	Connections between wireless networks and fixed networks should be treated in the same way as connections between fixed networks and the Internet
Recommended Control 17:	Wireless networks should be sufficiently segregated through the use of channel separation

When connecting devices via Ethernet to an agency's fixed network, agencies need to be aware of the risks posed by active wireless functionality. Devices may automatically connect to any open wireless networks they have previously connected to, which a malicious actor can use to masquerade and establish a connection to the device. This compromised device could then be used as a bridge to access the agency's fixed network. Disabling wireless functionality on devices, preferably by a hardware switch, whenever connected to a fixed network can prevent this from occurring. Additionally, devices do not have to be configured to remember and automatically

connect to open wireless networks that they have previously connected to. To ensure that a wireless network provided for public access cannot be used as a launching platform for attacks against an agency's system it must be segregated from all other systems. Security architectures incorporating segmented networks, DMZ's and other segregation mechanisms are useful in this regard. Wireless access points that have been certified in a Wi-Fi Alliance certification program provide an agency with assurance that they conform to wireless standards. Deploying wireless access points that are guaranteed to be interoperable with other wireless access points on a wireless network will limit incompatibility of wireless equipment and incorrect implementation of wireless devices by vendors.

A number of Extensible Authentication Protocol (EAP) methods, supported by the Wi-Fi Protected Access 2 (WPA2) protocol, are available.Ultimately, an agency's choice in authentication method will often be based on the size of their wireless deployment, their security requirements and any existing authentication infrastructure. If an agency is primarily motivated by security they can implement either PEAP-EAP-TLS or EAP-TLS. If they are primarily motivated by flexibility and legacy support they can implement EAP-TTLS. If they are primarily motivated by simplicity they can implement PEAP with EAP-MSCHAPv2.

To reduce the likelihood of a stolen smart card from being used to gain unauthorized access to a wireless network, two-factor authentication can be implemented through the use of Personal Identification Numbers (PINs) on smart cards. This is essential when a smart card grants a user any form of administrative access on a wireless network or attached network resource.

A security risk exists with EAP-TTLS and PEAP when a commercial certificate authority's certificates are automatically trusted by devices using vendor trusted certificate stores. This trust can be exploited by obtaining certificates from a commercial certificate authority under false pretenses, as devices can be tricked into trusting their signed certificate.

When 802.1X authentication is used, a shared secret key known as the Pairwise Master Key (PMK) is generated. Upon successful authentication of a device, the PMK can be cached to assist with fast roaming between wireless access points. When a device roams away from a wireless access point that it has authenticated to, it will not need to perform a full re-authentication should it roam back while the cached PMK remains valid. To further assist with roaming, wireless access points can be configured to pre-authenticate a device to other neighboring wireless access points that the device might roam to. Although requiring full authentication for a device each time it roams between wireless access points is ideal, agencies can chose to use PMK caching and pre-authentication if they have a business requirement for fast roaming. If PMK caching is used, the PMK caching period should not be set to greater than 1440 minutes (24 hours).

The use of pre-shared keys is poor practise and not recommended for wireless authentication, in common with many authentication and encryption mechanisms, the greater the length of pre-shared keys the greater the security they provide.

Administrative interfaces may allow users to modify the configuration and security settings of wireless access points. Often wireless access points by default allow users to access the administrative interface over methods such as fixed network connections, wireless network connections and serial connections directly on the device. Disabling the administrative interface on wireless access points will prevent unauthorized connections.

Effective DoS attacks can be performed on the 802.11 protocol by exploiting unprotected management frames using inexpensive commercial hardware. WPA2 provides no protection for management frames and therefore does not prevent spoofing or DoS attacks. 802.11w was ratified in 2009 and specifically addresses the protection of management frames on wireless networks. Wireless access points and devices should be upgraded to support the 802.11w amendment or any later amendment or version that includes a capability for the protection of management frames.

All wireless access points are configured with a default Service Set Identifier (SSID). The SSID is commonly used to identify the name of a wireless network to users. As the default SSIDs of wireless access points are well documented on online forums, along with default accounts and passwords, it is important to change the default SSID of wireless access points.When changing the default SSID, it is important that it lowers the profile of an agency's wireless network. In doing so, the SSID of a wireless network should not be readily associated with an agency, the location of or within their premises, or the functionality of the network.

The SSID of a wireless network shouldnot be readily associated with an agency, the premises, location or the functionality of the network.

Rogue devices or Access Points (APs) are unauthorized Wireless Access Points operating outside of the control of an agency. Assigning static IP addresses for devices accessing wireless networks can prevent a rogue device when connecting to a network from being assigned a routable IP address. However, some malicious actors will be able to determine IP addresses of legitimate users and use this information to guess or spoof valid IP address ranges for wireless networks. Configuring devices to use static IP addresses introduces a management overhead without any tangible security benefit.

Devices that connect to wireless networks have a unique Media Access Control (MAC) address. It is possible to use MAC address filtering on wireless access points to restrict which devices can connect to wireless networks. While this approach will introduce a management overhead of configuring whitelists of approved MAC addresses, it can prevent rogue devices from connecting to wireless networks. However, some malicious actors will be able to determine valid MAC addresses of

legitimate users already on wireless networks and use this information to spoof valid MAC addresses and gain access to a network. MAC address filtering introduces a management overhead without any real tangible security benefit.

When agency devices connect to non-agency controlled wireless networks, particularly public wireless networks, the devices may be exposed to viruses, malware or other malicious code. If any agency device becomes infected and is later connected to an agency controlled wireless network then a crossover of viruses, malware or malicious code could occur.

21.3. Video and Telephony Conferencing and Internet Protocol Telephony

Objective	**Video & Telephony Conferencing (VTC), Internet Protocol telephony (IPT) and Voice over Internet Protocol (VoIP) systems are implemented in a secure manner that does not compromise security, information or systems and that they operate securely**
Recommended Control 01:	Agencies should use a video, unified communication or voice-aware firewall that meets the same minimum level of assurance as specified for normal firewalls
Recommended Control 02:	Agencies should ensure that VTC and IPT functions can be established using only the secure signaling and data protocols
Recommended Control 03:	Agencies should: x configure VoIP phones to authenticate themselves to the call controller upon registration x disable phone auto-registration and only allow a whitelist of authorizeddevices to access the network x block unauthorized devices by default; x disable all unused and prohibited functionality x use individual logins for IP phones
Recommended Control 04:	Authentication should be enforced for: x registering a new phone x changing phone users x changing settings x accessing voice mail
Recommended Control 05:	Where an agency uses a VoIP phone in a lobby or shared area they should limit or disable the phone's: x ability to access data networks x functionality for voice mail and directory services
Recommended Control 06:	Agencies should use traditional analogue phones in lobby and shared areas
Recommended Control 07:	Agencies using softphones or webcams should install a host-based firewall on workstations utilizing softphones or webcams

Objective	**Video & Telephony Conferencing (VTC), Internet Protocol telephony (IPT) and Voice over Internet Protocol (VoIP) systems are implemented in a secure manner that does not compromise security, information or systems and that they operate securely**
	that allows traffic only to and from a minimum number of ports
Recommended Control 08:	Agencies should develop a Denial of Service response plan including: x how to identify the precursors and other signs of DoS x how to diagnose the incident or attack type and attack method x how to diagnose the source of the DoS x what actions can be taken to clear the DoS x how communications can be maintained during a DoS x report the incident
Recommended Control 09:	A Denial of Service response plan should include monitoring and use of: x router and switch logging and flow data x packet captures x proxy and call manager logs and access control lists x VTC and IPT aware firewalls and voice gateways x network redundancy x load balancing x PSTN failover x alternative communication paths

The use of video, unified communications and voice-aware firewalls ensures that only video or voice traffic (e.g. signaling and data) is allowed for a given call and that the session state is maintained throughout the transaction. The requirement to use a video, unified communication or voice-aware firewall does not necessarily require separate firewalls to be deployed for video conferencing, IP telephony and data traffic. If possible, agencies are encouraged to implement one firewall that is either video and data-aware; voice and data-aware; or video, voice and data-aware depending on their needs.

Use of secure signaling and data protects against eavesdropping, some types of DoS, man-in-the-middle and call spoofing attacks.

VTC equipment and VoIP phones need to be hardened and separated or segregated from the data network to ensure they will not provide an easy entry point to the network for an attacker.

An VTC or IPT DoS response plan will need to address the following:

- x how to identify the source of the DoS, either internal or external (location and content of logs)

- how to diagnose the incident or attack type and attack method
- how to minimize the effect on VTC or IPT, of a DoS of the data network (e.g. Internet or internal DoS), including separate links to other office locations for VTC and IPT and/or quality of service prioritization
- strategies that can mitigate the DOS (banning certain devices/Ips at the call controller and firewalls, implementing quality of service, changing VoIP authentication, changing dial-in authentication)
- alternative communication options (such as designated devices or personal mobile phones) that have been identified for use in case of an emergency

21.4. Intrusion Detection and Prevention

Objective	**An intrusion detection and prevention strategy is implemented for systems in order to respond promptly to incidents and preserve availability, confidentiality and integrity of systems**
Mandatory Control 01:	Agencies must select IDS / IPS that monitor uncharacteristic and suspicious activities
Mandatory Control 02:	When signature-based intrusion detection is used, agencies must keep the signatures and system patching up to date

Mandatory Control 03:	Agencies must:
	- develop and maintain a set of policies and procedures covering how to:
	  - minimise the likelihood of malicious code being introduced into a system
	  - prevent all unauthorised code from executing on an agency network
	  - detect any malicious code installed on a system
	- make their system users aware of the agency's policies and procedures
	- ensure that all instances of detected malicious code outbreaks are handled according to established procedures

Recommended Control 01:	Agencies should develop, implement and maintain an intrusion detection strategy that includes: - appropriate intrusion detection mechanisms, including network-based IDS/IPSs and host-based IDS/IPSs as necessary - the audit analysis of event logs, including IDS/IPS logs - a periodic audit of intrusion detection procedures - information security awareness and training programs - a documented IRP
Recommended Control 02:	Agencies should ensure sufficient resources are provided for the

Objective	**An intrusion detection and prevention strategy is implemented for systems in order to respond promptly to incidents and preserve availability, confidentiality and integrity of systems**
	maintenance and monitoring of IDS/IPS
Recommended Control 03:	Agencies should deploy IDS/IPSs in all gateways between the agency's networks and unsecure public networks or BYOD wireless networks
Recommended Control 04:	Agencies should deploy IDS/IPSs at all gateways between the agency's networks and any network not managed by the agency
Recommended Control 05:	Agencies should locate IDS/IPSs within the gateway environment, immediately inside the outermost firewall
Recommended Control 06:	In addition to agency defined configuration requirements, agencies should ensure that IDS/IPSs located inside a firewall are configured to generate a log entry, and an alert, for any information flows that contravene any rule within the firewall rule set
Recommended Control 07:	Agencies should test IDS/IPSs rule sets prior to implementation to ensure that they perform as expected
Recommended Control 08:	If a firewall is configured to block all traffic on a particular range of port numbers, the IDP/IPSs should inspect traffic for these port numbers and generate an alert if they are detected
Recommended Control 09:	Agencies should deploy tools for: x the management and archive of security event information x the correlation of suspicious events or events of interest across all agency networks
Recommended Control 10:	Agencies should use: x filters to block unwanted content and exploits against applications that cannot be patched x settings within the applications to disable unwanted functionality x digital signatures to restrict active content to trusted sources only

Malicious code can spread through a system from a number of sources including:

- x files containing macro viruses or worms
- x email attachments and Web downloads with malicious active content
- x executable code in the form of applications
- x security weaknesses in a system or network
- x security weaknesses in an application
- x contact with an infected system or media

The speed at which malicious code can spread through a system presents significant challenges and an important part of any defensive strategy is to contain the attack and limit damage.

If the firewall is configured to block all traffic on a particular range of port numbers, then the IDS should inspect traffic for these port numbers and alert if they are detected.

Generating alerts for any information flows that contravene any rule within the firewall rule set will assist security personnel in identifying and reporting to any possible breaches of agency systems.

In order to reduce the attack surface area of agency systems, it is good practice that agencies disable unused services and functions within network devices and operating systems. If agencies are deploying dual-stack equipment but not using the IPv6 functionality, then that functionality should be disabled. It can be re-enabled when required. This will reduce the opportunity to exploit IPv6 functionality before appropriate security measures have been implemented.

The information security implications around the use of IPv6 are still largely unknown and un-tested. As many of the deployed network protection technologies, such as firewalls and IDSs, do not consistently support IPv6, agencies choosing to implement IPv6 face an increased risk of systems compromise.

A number of tunneling protocols have been developed to facilitate interoperability between IPv4 and IPv6. Disabling IPv6 tunneling protocols when this functionality is not explicitly required will reduce the risk of bypassing network defenses by means of encapsulating IPv6 data inside IPv4 packets. Stateless Address Auto configuration (SLAAC) is a method of stateless IP address configuration in IPv6. SLAAC reduces the ability to maintain complete logs of IP address assignment on the network. To avoid this constraint, stateless IP addressing shouldnot be used.

Introducing IPv6 capable network devices into agency gateways can introduce a significant number of new security risks. Undergoing reaccreditation when new IPv6 equipment is introduced will ensure that any IPv6 functionality that is not intended to be used cannot be exploited by an attacker before appropriate information security mechanisms have been put in place. Once agencies have completed the transition to a dual-stack environment or completely to an IPv6 environment, reaccreditation will assist in ensuring that the associated information security mechanisms for IPv6 are working Gateway Security.

21.5. Gateways

Objective	**To ensure that gateways are properly configured to protect agency systems and information transferred between systems**

	from different security domains
Mandatory Control 01:	Agencies must perform a risk assessment on gateways and their configuration prior to their implementation.
Mandatory Control 02:	All domain and system owners connected through a gateway must understand and accept the residual security risk of the gateway and from any connected domains including those via a cascaded connection
Mandatory Control 03:	Agencies must limit access to gateway administration functions
Mandatory Control 04:	Agencies must ensure that system administrators are formally trained to manage gateways by qualified trainers
Mandatory Control 05:	Agencies must ensure that all system administrators of gateways that process GOB information meet the nationality requirements for these caveats
Mandatory Control 06:	Agencies must ensure that only authenticated and authorised system users can use the gateway
Mandatory Control 07:	Agencies must document any changes to gateways in accordance with the agency's Change Management Policy
Recommended Control 01:	Agencies should use demilitarized zones to house systems and information directly accessed externally
Recommended Control 02:	Agencies should annually review the security architecture of the gateway and risks of all connected domains including those via a cascaded connection
Objective	**To ensure that gateways are properly configured to protect agency systems and information transferred between systems from different security domains**
Recommended Control 03:	Once connectivity is established, domain owners should be considered information stakeholders for all connected domains
Recommended Control 04:	All system users should be trained in the secure use and security risks of the gateways before being granted access
Recommended Control 05:	Agencies should separate roles for the administration of gateways (e.g. separate network and security policy configuration roles)
Recommended Control 06:	Agencies should authenticate any IT equipment that connects to networks accessed through gateways
Recommended Control 07:	Agencies should undertake a risk assessment and update the SRMP before changes are implemented

Demilitarized zones are used to prevent direct access to information and systems on internal agency networks. Agencies that require certain information and systems to be accessed (Œ the Internet or some other form of remote access, should place them in the less trusted demilitarized zone instead of on internal agency networks.

Gateways could connect networks with different domain owners, including across agency boundaries. As a result, all domain and system owners must understand and accept the risks from all other networks before gateways are implemented.

Application of role separation and segregation of duties in administration activities will protect against security risks posed by a malicious system user with extensive access to gateways.

Authentication to networks as well as gateways can reduce the risk of unauthorized access and provide an audit capability to support the investigation of information security incidents.

Authenticating IT equipment to networks accessed through gateways will assist in preventing unauthorized IT equipment connecting to a network.

To avoid changes that may introduce vulnerabilities into a gateway, agencies should fully consider any changes and associated risks. Changes may also necessitate re-certification and accreditation of the system, see Chapter 7 - System Certification and Accreditation.

21.6. Firewalls

Objective	**Agencies operating bi-directional gateways implement firewalls and traffic flow filters to provide a protective layer to their networks in both discrete and virtual environments**
Mandatory Control 01:	All gateways must contain a firewall in both physical and virtual environments
Mandatory Control 02:	The requirement to implement a firewall as part of gateway architecture must be met independently by both parties (gateways) in both physical and virtual environments. (Shared equipment DOES not satisfy the requirements of this control)
Recommended Control 01:	Agencies should use a firewall of at least an EAL2 assurance level between a GOB network and another GOB controlled network within a single security domain

The higher the required assurance level for a firewall, the greater the assurance that it provides an appropriate level of protection against an attacker.

If a uni-directional connection between two networks is being implemented only one gateway is necessary with requirements being determined based on the source and destination networks. However, if a bi-directional connection between two networks is being implemented both gateways

will be configured and implemented with requirements being determined based on the source and destination networks.

As GOB networks are particularly sensitive, additional security measures need to be put in place when connecting them to other networks.

21.7. Diodes

Objective	**Networks connected to one-way (uni-directional) gateways implement diodes in order to protect the higher classified system**
Mandatory Control 01:	Agencies must use a diode of at least an EAL2 assurance level between an GOB network and a foreign network
Recommended Control 01:	Agencies should use a diode of at least an EAL2 assurance level between an GOB network and another Bangladesh controlled network within a single security domain
Recommended Control 02:	Agencies deploying a diode to control data flow within one-way gateways should monitor the volume of the data being transferred

Monitoring the volume of data being transferred across a diode will ensure that it conforms to expectations. It can also alert the agency to potential malicious activity if the volume of data suddenly changes from the norm.

21.8. Session Border Controller

Objective	**To ensure the use of Session Border Controllers (SBCs) is integrated with the agency's security architecture and that use is consistent with other requirements for gateway security in this chapter**
Mandatory Control 01:	Agencies must use a diode of at least an EAL2 assurance level between an GOB network and a foreign network
Mandatory Control 02:	Agencies intending to adopt VoIP or UC technologies or services must consider the risks to the availability of systems and information in their design of VoIP and UC systems architecture, fault tolerance, fail over and supporting controls and governance processes
Mandatory Control 03:	Agencies intending to adopt VoIP or UC technologies or services must conduct a comprehensive risk assessment before implementation or adoption
Mandatory Control 04:	Agencies must ensure risks for any VoIP or UC service adopted are