What have we done, procedures processes and policies in place?

What are we going to do, procedures, processes and policies to be put in place?

Owner?

Updates?

Lessons Learnt?

CMM Detail:

LEADERSHIP AND CULTURE

Executive commitment and governance

GOV 1 - Agencies must establish a governance structure within their agency that ensures the successful management of protective security risk.

GOV 2 - Agencies must appoint a member of senior management as the Chief Security Officer (CSO), responsible for the agency protective security policy and oversight of protective security practices.

GOV 10 - Agencies must establish a business continuity management (BCM) programme to provide for the continued availability of critical services and assets, and of other services and assets when warranted by the security threat or risk assessment.

Management structure, roles and responsibilities

GOV 1 - Agencies must establish a governance structure within their agency that ensures the successful management of protective security risk.

GOV 2 - Agencies must appoint a member of senior management as the Chief Security Officer (CSO), responsible for the agency protective security policy and oversight of protective security practices.

Monitoring and assurance

GOV 4 - Agencies must develop their own set of protective security policies, plans and protocols to meet their specific business needs. Policies and plans must be reviewed every two years or sooner if changes in risks or agency's operating environment dictate.

GOV 5 - Agencies must have an assurance system to conduct an annual security assessment against the mandatory requirements detailed within the Protective Security Requirements. Agencies must be prepared to report this assessment information upon request from lead security agencies.

Organisation culture and behaviour

GOV 6 - Agencies must provide all staff, including contractors, with sufficient information and security awareness training to meet the obligations of the Protective Security Requirements.

GOV 7 - Agencies must have established procedures for reporting and investigating security incidents, and for taking corrective action.

GOV 8 - Agencies must ensure contracted providers comply with the Protective Security Requirements and agency specific protective security protocols.

PHYSEC 2 - Agencies must have in place policies and protocols to:
- identify, protect and support employees under threat of violence, based on a threat and risk assessment of specific situations. In certain cases agencies may have to extend protection and support, for example to family members.
- report incidents to management, human resources, security and law enforcement authorities, and/or Work safe NZ as appropriate.
- provide information, training and counselling to employees
- maintain thorough records and statements on reported incidents.

Education and communications

GOV 6 - Agencies must provide all staff, including contractors, with sufficient information and security awareness training to meet the obligations of the Protective Security Requirements.

GOV 9 - Agencies must adhere to any provisions concerning the security of people, information and assets contained in multilateral or bilateral agreements and arrangements to which New Zealand or the agency is a party.

PHYSEC 1 - Agencies must provide clear direction on physical security through the development and implementation of an agency physical security policy, and address agency physical security requirements as part of the overall agency security plan.

PHYSEC 2 - Agencies must have in place policies and protocols to:
- identify, protect and support employees under threat of violence, based on a threat and risk assessment of specific situations. In certain cases agencies may have to extend protection and support, for example to family members.
- report incidents to management, human resources, security and law enforcement authorities, and/or Work safe NZ as appropriate.
- provide information, training and counselling to employees
- maintain thorough records and statements on reported incidents.

PLANNING, POLICIES AND PROTOCOLS

Strategy development and delivery

GOV 3 - Agencies must adopt a risk management approach to cover all areas of protective security activity across their organisation, in accordance with the New Zealand standard AS/NZS ISO 31000:2009 Risk Management - Principles and Guidelines.

GOV 4 - Agencies must develop their own set of protective security policies, plans and protocols to meet their specific business needs. Policies and plans must be reviewed every two years or sooner if changes in risks or agency's operating environment dictate.

GOV 5 - Agencies must have an assurance system to conduct an annual security assessment against the mandatory requirements detailed within the Protective Security Requirements. Agencies must be prepared to report this assessment information upon request from lead security agencies.

GOV 10 - Agencies must establish a business continuity management (BCM) programme to provide for the continued availability of critical services and assets, and of other services and assets when warranted by the security threat or risk assessment.

Policies, processes and procedures

GOV 4 - Agencies must develop their own set of protective security policies, plans and protocols to meet their specific business needs. Policies and plans must be reviewed every two years or sooner if changes in risks or agency's operating environment dictate

GOV 6 - Agencies must provide all staff, including contractors, with sufficient information and security awareness training to meet the obligations of the Protective Security Requirements.

GOV 8 - Agencies must ensure contracted providers comply with the Protective Security Requirements and agency specific protective security protocols.

GOV 9 - Agencies must adhere to any provisions concerning the security of people, information and assets contained in multilateral or bilateral agreements and arrangements to which New Zealand or the agency is a party.

GOV 10 - Agencies must establish a business continuity management (BCM) programme to provide for the continued availability of critical services and assets, and of other services and assets when warranted by the security threat or risk assessment.

PERSEC 1 - Agencies must ensure New Zealand government employees, contractors and temporary staff who require ongoing access to New Zealand government information and resources:
- are eligible to have access
- have had their identities established
- are suitable to have access, and
- are willing to comply with government policies, standards, protocols and requirements that safeguard that agency's resources (people, information and assets) from harm.
Agencies must have in place policies and procedures to assess and manage the ongoing suitability for employment of all staff and contractors.

PERSEC 6 - Agencies must have personnel security clearance management arrangements in place for all staff, including contractors, who hold a security clearance.

INFOSEC 1 - Agencies must address information security requirements through the development and implementation of an information security policy as part of the agency security plan.

INFOSEC 2 - Agencies must establish a framework to provide direction and coordinated management of information security.

INFOSEC 3 - Agencies must implement policies and protocols for the protective marking and handling of information assets in accordance with the Protective Security Requirements New Zealand Government Security Classification System and the New Zealand Information Security Manual.

PHYSEC 1 - Agencies must provide clear direction on physical security through the development and implementation of an agency physical security policy, and address agency physical security requirements as part of the overall agency security plan.

PHYSEC 2 - Agencies must have in place policies and protocols to:
- identify, protect and support employees under threat of violence, based on a threat and risk assessment of specific situations. In certain cases agencies may have to extend protection and support, for example to family members.
- report incidents to management, human resources, security and law enforcement authorities, and/or Work safe NZ as appropriate.

- provide information, training and counselling to employees
- maintain thorough records and statements on reported incidents.

Risk management

GOV 3 - Agencies must adopt a risk management approach to cover all areas of protective security activity across their organisation, in accordance with the New Zealand standard AS/NZS ISO 31000:2009 Risk Management - Principles and Guidelines.

GOV 10 - Agencies must establish a business continuity management (BCM) programme to provide for the continued availability of critical services and assets, and of other services and assets when warranted by the security threat or risk assessment.

PERSEC 6 - Agencies must have personnel security clearance management arrangements in place for all staff, including contractors, who hold a security clearance.

INFOSEC 2 - Agencies must establish a framework to provide direction and coordinated management of information security. Frameworks must be appropriate to the level of security risk in the agency's information environment and consistent with business needs and legal obligations.

INFOSEC 5 - Agencies must ensure there is a formal process to approve ICT system to operate. This process, known as 'credification and accreditation', is an essential component of the governance and assurance of ICT systems and supports risk management. The process is described in the New Zealand Information Security Manual.

PHYSEC 6 - Agencies must implement a level of physical security measures that minimise or remove the risk of information assets being made inoperable or inaccessible, or improperly accessed or used.

Incident management

GOV 7 - Agencies must have established procedures for reporting and investigating security incidents, and for taking corrective action.

PHYSEC 2 - Agencies must have in place policies and protocols to:
- identify, protect and support employees under threat of violence, based on a threat and risk assessment of specific situations. In certain cases agencies may have to extend protection and support, for example to family members.
- report incidents to management, human resources, security and law enforcement authorities, and/or Work safe NZ as appropriate.
- provide information, training and counselling to employees
- maintain thorough records and statements on reported incidents.

SECURITY DIMENSIONS

Personnel Security

GOV 3 - Agencies must adopt a risk management approach to cover all areas of protective security activity across their organisation, in accordance with the New Zealand standard AS/NZS ISO 31000:2009 Risk Management - Principles and Guidelines.

GOV 6 - Agencies must provide all staff, including contractors, with sufficient information and security awareness training to meet the obligations of the Protective Security Requirements.

GOV 8 - Agencies must ensure contracted providers comply with the Protective Security Requirements and agency specific protective security protocols.

PERSEC 1 - Agencies must ensure New Zealand government employees, contractors and temporary staff who require ongoing access to New Zealand government information and resources:
- are eligible to have access
- have had their identities established
- are suitable to have access, and
- are willing to comply with government policies, standards, protocols and requirements that safeguard that agency's resources (people, information and assets) from harm.

Agencies must have in place policies and procedures to assess and manage the ongoing suitability for employment of all staff and contractors.

PERSEC 2 - Agencies must:
- identify positions within their agency that require access to CONFIDENTIAL, SECRET and TOP SECRET assets and information
- ensure the level of security clearance sought is necessary, and
- ensure personnel have the requisite level of security clearance prior to being granted access to information protectively marked as CONFIDENTIAL or higher.

PERSEC 3 - Agencies must maintain a register of personnel and contractors who hold a security clearance.

PERSEC 4 - An application for a security clearance must be sponsored by a New Zealand government agency.

PERSEC 5 - Agency heads must obtain a recommendation from the NZSIS prior to granting a security clearance. Agencies must follow the Protective Security Requirements Personnel Security Management Protocol and supporting requirements for personnel security.

PERSEC 6 - Agencies must have personnel security clearance management arrangements in place for all staff, including contractors, who hold a security clearance.

PERSEC 7 - Agencies must notify the NZSIS of the granting, downgrading, suspension or cancellation of a security clearance. Any reason associated with disciplinary action or unsuitability of the candidate to obtain/maintain the appropriate level of clearance must be reported to the NZSIS.

Information security

GOV 3 - Agencies must adopt a risk management approach to cover all areas of protective security activity across their organisation, in accordance with the New Zealand standard AS/NZS ISO 31000:2009 Risk Management - Principles and Guidelines.

GOV 10 - Agencies must establish a business continuity management (BCM) programme to provide for the continued availability of critical services and assets, and of other services and assets when warranted by the security threat or risk assessment.

INFOSEC 1 - Agencies must address information security requirements through the development and implementation of an information security policy as part of the agency security plan.

INFOSEC 2 - Agencies must establish a framework to provide direction and coordinated management of information security. Frameworks must be appropriate to the level of security risk in the agency's information environment and consistent with business need

INFOSEC 3 - Agencies must implement policies and protocols for the protective marking and handling of information assets in accordance with the Protective Security Requirements New Zealand Government Security Classification System and the New Zealand Information Security Manual.

INFOSEC 4 - Agencies must document and implement operational procedures and measures to ensure information, systems development and systems operations are designed and managed in accordance with security, privacy, legal and regulatory obligations under which the agency operates.

INFOSEC 5 - Agencies must ensure there is a formal process to approve ICT system to operate. This process, known as 'credification and accreditation', is an essential component of the governance and assurance of ICT systems and supports risk management. The process is described in the New Zealand Information Security Manual.

Physical security

GOV 3 - Agencies must adopt a risk management approach to cover all areas of protective security activity across their organisation, in accordance with the New Zealand standard AS/NZS ISO 31000:2009 Risk Management - Principles and Guidelines.

GOV 6 - Agencies must provide all staff, including contractors, with sufficient information and security awareness training to meet the obligations of the Protective Security Requirements.

GOV 8 - Agencies must ensure contracted providers comply with the Protective Security Requirements and agency specific protective security protocols.

PHYSEC 1 - Agencies must provide clear direction on physical security through the development and implementation of an agency physical security policy, and address agency physical security requirements as part of the overall agency security plan.

PHYSEC 2 - Agencies must have in place policies and protocols to:
- identify, protect and support employees under threat of violence, based on a threat and risk assessment of specific situations. In certain cases agencies may have to extend protection and support, for example to family members.
- report incidents to management, human resources, security and law enforcement authorities, and/or Work safe NZ as appropriate.
- provide information, training and counselling to employees
- maintain thorough records and statements on reported incidents.

PHYSEC 3 - Agencies must ensure they fully integrate physical security early in the process of planning, selecting, designing and modifying their facilities.

PHYSEC 4 - Agencies must ensure any proposed physical security measures or activity is consistent with relevant employer occupational health and safety obligations.

PHYSEC 5 - Agencies must show a duty of care for the physical safety of members of the public interacting directly with the New Zealand government. Where an agency's function involves providing services, the agency must ensure clients can transact with the New Zealand government with confidence about their physical wellbeing.

PHYSEC 6 - Agencies must implement a level of physical security measures that minimise or remove the risk of information assets being made inoperable or inaccessible, or improperly accessed or used.

PHYSEC 7 - Agencies must develop plans and protocols to move up to heightened security levels in case of emergency and increased threat. The New Zealand Government may direct its agencies to implement heightened security levels.