PSR annual self-assessment assurance process Guidance on additional INFOSEC questions

October 2019

Strengthening Information Assurance

On 8 December 2014, Cabinet approved the Protective Security Requirements (PSR), which incorporates the New Zealand Information Security Manual (NZISM). Mandated agencies are required to comply with the baseline requirements of the NZISM. These baseline requirements are the minimum level of protections your agency needs to put in place, to meet compliance with the NZISM.

This reporting period, the PSR annual self-assessment assurance process includes additional questions focused on INFOSEC which you will need to answer in order to complete your assessment. Once completed, the additional information will provide you and your CE with greater visibility of the INFOSEC posture of your agency, and help you focus on those INFOSEC areas where a more concentrated effort may be required. It will also allow the GCISO to identify systemic issues, and better assess what is needed from the centre to help provide overall uplift for INFOSEC.

This document provides guidance on what good information security should look like, in response to the additional INFOSEC questions. This guidance is aligned with the NZISM, and recognised international information security frameworks. It also points agencies to their obligations under the Protective Security Requirements PSR Framework.

The following guidance has been developed to help agencies to better understand their assurance posture and improve their INFOSEC capability and maturity.

Overview

Information security is becoming increasing complex for agencies as technologies continue to evolve. It can be challenging to keep abreast of the risks associated with them. Managing information security risk is key to ensuring the protection of your agency's critical information assets and the retention of public trust and confidence.

Information security needs to be approached as more than "just an IT issue" – it needs to be treated as business risk, with the key question being, if an INFOSEC risk eventuates, what impact will it have on the organisation's reputation, your customers, or your stakeholders?

As a security lead for your agency, you are accountable for ensuring your agency is effectively managing information security risk and reporting such risks to your CE. Your agency should have an assurance plan which ensures you receive regular reporting on how the information security risks within your organisation are being managed.

You need to have regular engagement with your senior leadership team, and with those who are responsible for ensuring your agency's risk tolerance is managed to an accepted level. You and your senior leadership team should have clear understanding and visibility of your agencies INFOSEC assurance posture to be able to effectively to manage the risks.

Governance

As CISO, do you understand where the responsibility for your organisation's INFOSEC governance should rest?

The chief executive or agency head is required to endorse, and is accountable for, information security within their agency. If an information security incident occurs, ultimately it is they who are held accountable. Information systems governance is the responsibility of the agency head and the executive team.

Leadership, organisational structures, and processes ensure that the agency's information systems support and sustain the both the agency's, and governments, objectives. Systems within your agency should have an owner to ensure that IT governance processes are followed, and that business requirements can be met. System owners should be members of the executive team, especially for critical agency systems.

Does your organisation have a formal decision making body to which INFOSEC issues are formally raised?

Information security risks and issues should be communicated through a formal steering committee or advisory board for consideration. Such a decision making body should comprise key business and IT executives, and should meet regularly. Your senior leadership team should be provided with regular reporting and updates from this group. Reporting needs to be meaningful and aligned with business objectives.

The coordination of information security risk management, between the business and information security teams, should be led by the CISO to ensure the alignment of business and security objectives within the agency.

Information Security Policy

Are your Information Security and Information Management policies aligned with your organisation's mission?

Sound information security policies are an essential part of security, as they both demonstrate and support good governance practices. Information security policies outline the high-level objectives for your agency's information security.

Agencies are required to have an information security policy. Information security policies are an aggregate of rules and practices that prescribe how your agency manages and protects its information.

Policies and procedures should be established and maintained in support of data security. They should include measures that support the confidentiality, integrity, and availability of information across multiple system interfaces, jurisdictions, and business functions, in order to prevent the improper disclosure, alteration, or destruction of information.

Security documentation may be incorporated within wider agency policies. So long as the policy and its intent are clear and discoverable, this is an acceptable practice.

Infrastructure (Building in Security by Design)

How do you ensure that security is factored into system architecture?

A risk assessment is required to be conducted and documented before creating architecture and designing an agency network. The principles of security architecture in the NZISM should be built into your network design. This will maximise design and operational efficiency, and provide essential security support to the system.

Large systems are difficult to protect, and are also difficult to monitor and control when it comes to ensuring that the security controls that have been implemented are effective.

Sufficient security consideration needs to be given to each individual component feeding into a system and how it works, as some controls may stop the system from operating securely. The use of New Zealand Government-approved products is encouraged, as they provide higher levels of assurance in regard to security considerations.

Is this included in your project methodology?

System security can be optimised by ensuing it is built in at the design phase. There needs to be a balanced approach to security, and the design should include both proactive and reactive loss prevention strategies. Such an approach will ensure that stakeholders are assured that a newly-built system has sufficient security embedded within it, to both protect information assets and support business objectives.

The design, acquisition, implementation, configuration, modification, and management of infrastructure and software should be well defined in both security policies and project documentation to prevent security incidents.

Certification and Accreditation

Please outline the strategy/plan you have in place for the certification of existing systems, including business-critical assets that require ongoing recertification?

Certification is an essential component of the governance and assurance processes. It addresses issues and supports the risk management of information security systems. Certification involves the testing and evaluation of the technical and nontechnical security features of a system, to determine its compliance with a set of specified security requirements. Accreditation is the formal acceptance of the risks associated with a system.

Certification and accreditation should enable you to link the organisation's risk management processes to its business objectives. This will guide you in establishing who is accountable for the controls implemented within an organisation's information systems.

How do you prioritise this work?

The implementation of continuous monitoring processes provides senior leaders and the executive with the necessary information to make efficient, cost-effective, risk-informed decisions about the systems supporting the organisation's mission. This allows agencies to incorporate security and privacy into the system development life cycle and business functions.

Conducting on-going monitoring of information security systems will assist the agency in assessing any changes to the environment or to their operations. This will help determine the implications for a system if its security risk profile was to change.

Incidents

Describe your planning for INFOSEC and cyber security incident response. How regularly is it tested?

Incident response plans ensure that information security incidents are appropriately managed and contained, to prevent them from escalating.

Agencies need to develop an incident response plan and supporting procedures, and these should be tested regularly. When significant organisational or environmental change occurs plans also need to be tested to ensure they are still fit for purpose. This also ensures that agency personnel are familiar with the execution of the plan.

Incident response plans, and their testing, need to involve impacted customers, existing business relationships and those in your supply chain who may have dependencies on the impacted system. Testing should also include when and who should formally report an incident to the correct authority.

It is desirable to review your technical controls after an incident to ensure they are fit for purpose, and then retest the plan to ensure its suitability in guiding your response to incidents.

Access Controls

Do you have separate policies and processes in place to specifically manage all users (including contractors and third parties) with privileged access to systems?

Policies to manage access controls need to be implemented, to ensure access rights to all systems can be effectively managed and monitored.

User access policies and procedures need to be established for employees, contractors, and third-party users, along with supporting business processes and technical measures. This ensures that identity, entitlement, and access management for all users with access to data is appropriately managed.

Access control policies need to include the management of system accounts, group memberships, and elevated privileges. Privileged access rights can allow users to make system-wide changes. The inappropriate use of privileged user credentials within a system or application can be a major factor contributing to failures, information security incidents, or system breaches.

The use of appropriate and effective mechanisms to log the activities of privileged users, together with strong change management practices, will provide greater accountability and auditing capability to agency IT systems.

Do you have appropriate on boarding and off boarding controls around privileged access?

The timely de-provisioning of all user access to data, applications, infrastructure systems, and network components, should be implemented and should follow the principle of least privilege based on job function.

Roles and responsibilities for performing employment termination or change in employment procedures need to be assigned, documented, and communicated.

Monitoring and Maintaining Information Systems and Assets

How do you undertake risk monitoring, ensure it is fit for purpose, supports assurance, and is communicated to decision makers?

Information assets should be classified and understood in terms of business criticality, service-level expectations, and operational continuity requirements. They should be assigned an owner with defined roles and responsibilities.

Reviews can be scoped according to specific requirements. They should be conducted by an independent person or third-party at least annually, and the results must be documented. This will ensure that the organisation addresses any issues identified in relation to existing policies, standards, procedures, and compliance obligations. These results should be reported to your agency's risk committee and/or governance board.

An effective information security governance program requires constant review. Agencies should monitor the status of their programs of work to ensure that:

- Information security activities provide appropriate support to the agency mission;
- Policies and procedures are current, updated regularly and aligned with evolving technologies where required;
- Controls are effective, and are working as intended.

Developing an audit plan will ensure that the security posture of your systems is maintained. This will lessen the risk of disruption to your business objectives. Plans should be focused on reviewing the effectiveness of the implementation of security operations. Audit activities need to be agreed upon prior to proceeding with any audits, to ensure they do not disrupt business processes.

Information Security – Supply Chain Management

How often do you review your supply chain so that any risks are identified and adequately mitigated?

Technology supply chains are established and managed to ensure the continuity of supply and the protection of sensitive information.

Supply chains are complex. They can be globally distributed, and often involve interconnected sets of resources and processes linking multiple organisations.

ICT supply chains can introduce particular risks to an agency and supply chain risk management is a critical organisational function. Supply chain risks should be monitored on an on-going basis, and controls and mitigations adjusted accordingly. They should be incorporated into the organisation's

wider risk assessment and management processes. This allows them to be managed appropriately through the procurement process, and through technical checks and controls.

Independent reviews and assessments should be performed at least annually, to ensure that the organisation addresses any lack of adherence to policies, standards, procedures, and compliance obligations, so these can be managed.

Supply chain policies and procedures in relation to information security should support business processes and technical measures that have been implemented. These should ensure that all system components have been pre-authorised by the organisation's leadership, and that governance functions have been appropriately carried out. To reduce the risk in your supply chain, your agency should follow the Government Rules of Procurement.

Policies and procedures need to be implemented to ensure the consistent review of service agreements across the relevant supply chains. Reviews should be performed regularly and must identify any lack of adherence to established agreements.

Contracts

How INFOSEC requirements are built into procurement and contractual agreements and how is this monitored and enforced?

Contracts should outline the roles and responsibilities of those involved in organisational IT security services, for both the organisation and the supplier.

The level of control over your systems is usually established by the terms and conditions of the contracts or service-level agreements with external service providers, and can range from extensive to very limited control.

Agreements and contracts between providers and organisations should incorporate at least the following mutually-agreed information security-related clauses and terms:

- The primary points of contact for the duration of the business relationship for both the provider and customer;
- Details regarding support for any relevant business processes and the specific technical measures being implemented;
- Descriptions of any governance, risk management, and assurance requirements, and any legal, statutory and regulatory compliance obligations;
- Details concerning what happens to information and customer data held by the provider at the expiration of the relationship;
- Details concerning the timely notification of a security incident (or confirmed breach) to all customers, and any other stakeholders that are impacted; and
- How the authorisation of any changes controlled by the provider will be managed, where it impacts the customer.

Considering Jurisdictional Risks

Can you provide an accurate view of the extent to which your data and IT infrastructure is hosted off shore?

The agency's leadership team needs to understand and have visibility over where the agency's information and IT infrastructure physically reside. This includes those parties that may have access to any of the organisation's information that is held in foreign jurisdictions, and the provision of support services for infrastructure hosted offshore. This information should inform the organisation's risk assurance, business continuity, and disaster recovery processes, and how security is prioritised.

Formal approval, review and audit processes for the use of new and existing applications and technologies need to be established, to ensure any associated jurisdictional risk has been considered. This will reduce the risk of unsanctioned IT applications and technologies that potentially harbour unknown vulnerabilities operating within the organisation's wider IT environment. It will also reduce the risk of sensitive information being exposed to unauthorised parties.