4.3. Conducting Audits

Objective

4.3.1. The effectiveness of information security measures for systems is periodically reviewed and validated.

Context

Scope

4.3.2. This section covers information on the process of undertaking a certification and accreditation audit.

Audit objectives, scope and criteria

4.3.3. The aim of an audit is to review and assess:

- the risk identification and assessment;
- design and complexity (including the system and security architectures);
- any available assurance reports on support or outsourced services;
- controls selection;
- actual implementation and effectiveness of controls for a system; and
- supporting information security documentation.

4.3.4. Only information that is verifiable should be accepted as audit evidence. Audit evidence should be recorded.

Audit outcome

4.3.5. 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.

4.3.6. Part of this audit is an assessment of whether the control systems adequately identify and address risk and information security requirements.

Who can assist with an audit

4.3.7. A number of other agencies and personnel within agencies are often consulted during an audit. Agencies or personnel that can be consulted on physical security aspects of information security may include:

- The NZSIS for Physical Security;
- GCSB for TOP SECRET sites and Sensitive Compartmented Information Facilities (SCIFs);
- MFAT for systems located at overseas posts and missions;
- The Chief Security Officer (CSO) may be consulted on personnel and physical security aspects of information security;
- The CISO, ITSM or communications security officer may be consulted on COMSEC aspects of information security; and
- The ITSM and System Owner on aspects of secure system design configuration and operation.

Independent audits

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

Audit Evidence

4.3.9 Audit evidence can be obtained from documentation described in Chapter 5 – Information Security Documentation.

Other sources may include:

Source	
Agency Strategies and Statements of Intent.	Any additional process documentation referenced in the documentation described in the NZISM Chapter 5.
Third party service provider agreements.	Independent risk assessments or security evaluations, such as penetration tests by an internal team or an external organization.
The agency risk identification and assessment process.	Any internal audit reports, assessments and reviews.
Any statements of applicability.	Any relevant incident reports.

Audit evidence reliability

4.3.10. The reliability of audit evidence is influenced by its source, nature and the circumstances under which the evidence is gathered. In general terms documentary evidence is more reliable than oral evidence, self-generated evidence less reliable than evidence gathered elsewhere and externally generated evidence is more reliable than internally generated evidence as internally generated evidence may be more susceptible to selective presentation.

4.3.11. Confirmation should be obtained that:

- Risk owners have been identified; and
- Each risk owner has sufficient accountability and authority to manage their identified risks.

4.3.12. Audit evidence can be gathered through the following methods in order of preference:

Method	Description
Inspection	Physical inspections can provide an independent confirmation of the physical condition of the site or systems, its implementation and its management.
Analytical review	Reviews of records and documents will provide evidence of varying degrees of reliability depending on their nature and source. A review of the risk identification and selection of risk treatments is invaluable.
Enquiry	Here audit evidence is gathered by interview. Enquiries can be formal or informal and oral or written. It is essential that the auditor creates a written record of any enquiries conducted.
Observation	Observation of operations or procedures being performed by others with the aim of determining the manner of its performance only at that particular time. This may include checks on system configurations, change management processes or other key elements.
Computations	Rarely used for non-financial records but may include, for example, asset registers and validation of holdings of accountable equipment and software.

Audit evidence sufficiency

4.3.13. The Sufficiency is the measure of the quality (not the quantity) of audit evidence. It is important, however, that a balance is struck between the extent of the audit, the nature of the system under review, agency risk and the cost, effort and benefit of the audit. Sufficient evidence should be obtained to allow the auditor to be able to draw reasonable conclusions on which to base the audit opinion. For evidence to be deemed sufficient, the following aspects should be considered:

- Materiality. Materiality is the threshold where any distorted, missing and incorrect information is likely to have an impact on the risk and security of a system. Where it becomes clear that there are material deficiencies in the evidence presented more substantive tests may be required or the audit suspended until corrective action has been taken by the agency.
- Risk assessment: It is almost impossible to validate every risk identification and selection of risk treatments. For larger systems a more practical approach may be to validate the identification and treatment of major risks and use sampling techniques for the balance.
- Economy: Before gathering or requesting additional audit evidence, it is important to consider whether or not it is feasible or cost-effective to generate this evidence against the benefits, assessed value and time required.

References

4.3.14. Further references can be found at:

Reference	Title	Publisher	Source
AS/NZ ISO 19011:2019	**Guidelines for auditing management systems**	Standards NZ	https://standards.govt.nz/
ISO 19011:2018	**Guidelines for auditing management systems**	ISO	https://www.iso.org/standard/70017.html
ISO/IEC 27000:2018	**Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary**	ISO	https://www.iso.org/standard/73906.html
ISO/IEC 27001:2013	**Information technology -- Security techniques -- Information security management systems -- Requirements**	ISO	https://www.iso.org/standard/54534.html
ISO/IEC 27002:2022	**Information security, cybersecurity and privacy protection — Information security controls**	ISO	https://www.iso.org/standard/75652.html
ISO/IEC 27006:2015	**Information Technology – Security Techniques- Requirements for bodies providing audit and certification of information security management systems**	ISO	https://www.iso.org/standard/62313.html
ISO/IEC 27007:2020	**Information Technology – Security Techniques - Guidelines for information security management systems auditing**	ISO	https://www.iso.org/standard/77802.html
International Standard On Auditing (New Zealand) 500	**Audit Evidence**	External Reporting Board, NZ Audit and Assurance Standards Board	https://xrb.govt.nz/standards-for-assurance-practitioners/auditing-standards/isa-nz-500/

PSR references

4.3.15.

Reference	Title	Source
PSR Mandatory Requirements	GOV3, GOV8, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements
PSR content protocols	Management protocol for information security	Management protocol for information security | Protective Security Requirements
PSR requirements sections	Self assessment & reporting	Self-assessment and reporting | Protective Security Requirements
Managing specific scenarios	Managing specific scenarios | Protective Security Requirements	Transacting online with the public

Rationale & Controls

Independence of auditors

4.3.16.R.01. **Rationale**

As there can be a perceived conflict of interest in the system owner assessing the security of their own system it is important that the auditor is demonstrably independent. This does not preclude an appropriately qualified system owner from assessing the security of a system that they are not responsible for.

4.3.16.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:562]

Agencies SHOULD ensure that auditors conducting audits are able to demonstrate independence and are not also the system owner or certification authority.

Audit preparation

4.3.17.R.01. **Rationale**

Ensuring that the system owner has approved the system architecture and associated information security documentation will assist auditors in determining the scope of work for the first stage of the audit.

4.3.17.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:565]

Prior to undertaking the audit the system owner MUST approve the system architecture and associated information security documentation.

Audit (first stage)

4.3.18.R.01. **Rationale**

Auditing against the risk assessment and subsequent controls selection is preferable to a 'checklist' approach where all controls in the NZISM are checked for selection and implementation irrespective of applicability.

4.3.18.R.02. **Rationale**

The purpose of the first stage of the audit is to determine that the system and security architecture (including information security documentation) is based on sound information security principles and has addressed all **applicable** controls from this manual. During this stage the statement of applicability for the system will also be assessed along with any justification for non-compliance with applicable controls from this manual.

4.3.18.R.03. **Rationale**

Without implementing the controls for a system their effectiveness cannot be assessed during the second stage of the audit.

4.3.18.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:569]

The SecPol, SRMP, SSP, 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.

4.3.18.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:570]

The Information Security Policy (SecPol) MUST be reviewed by the auditor to ensure that all applicable controls specified in this manual are addressed.

4.3.18.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:571]

The system and security architecture (including information security documentation) SHOULD be reviewed by the auditor to ensure that it is based on sound information security principles and meets information security requirements, including the NZISM.

4.3.18.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:572]

The Information Security Policy (SecPol) SHOULD be reviewed by the auditor to ensure that policies have been developed or identified by the agency to protect classified information that is processed, stored or communicated by its systems.

4.3.18.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:573]

The system owner SHOULD provide a statement of applicability for the system which includes the following topics:

- the baseline of this manual used for determining controls;
- controls that are, and are not, applicable to the system;
- controls that are applicable but are not being complied with; and
- any additional controls implemented as a result of the SRMP.

Implementing controls

4.3.19.R.01. **Rationale**

System testing is most effective on working systems. Desk checks have limited effectiveness in these situations.

4.3.19.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:576]

Prior to undertaking any system testing in support of the certification process, the system owner MUST implement the controls for the system.

Audit (second stage)

4.3.20.R.01. **Rationale**

The purpose of the second stage of the audit is to determine whether the controls, as approved by the system owner and reviewed during the first stage of the audit, have been implemented correctly and are operating effectively.

4.3.20.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:579]

The implementation of controls MUST be assessed to determine whether they have been implemented correctly and are operating effectively.

4.3.20.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:580]

The auditor MUST ensure that, where applicable, a physical security certification has been awarded by an appropriate physical security certification authority.

4.3.20.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:581]

The physical security certification SHOULD be less than three (3) years old at the time of the audit.

Report of compliance

4.3.21.R.01. **Rationale**

The report of compliance assists the certification authority in conducting a residual security risk assessment to assess the residual security risk relating to the operation of a system following the audit and any remediation activities the system owner may have undertaken.

4.3.21.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:584]

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.