5.8. Independent Assurance Reports

Objective

5.8.1. To provide assurance to System Owners, Certifiers, Practitioners and Accreditors and to assist system designers, enterprise and security architects where assurance reviews cannot be directly undertaken on service providers.

Context

Scope

5.8.2. Independent assurance reports are also variously referred to as third party assurance reporting, third party reviews, attestation reports and SAS 70 reports. It is important to note that SAS 70 has been superseded by the ISAE 3402 and SSAE 16 standards encompassing Type I and 2 and SOC 1, 2 and 3 reports. For reviews conducted in New Zealand the ISAE (NZ) 3402 or ISAE (NZ) 3000 standards are used. These various standards and report types are discussed later in this section. Agencies are likely to encounter a variety of report types, depending on the country of residence or country of jurisdiction of the service provider, or the geographic location of the data centre.

Purpose

5.8.3. Many organisations are outsourcing key components of their business such as telecommunications, data storage and cloud based services. Managing third-party relationships is particularly challenging with services provided from outside New Zealand. The global nature of these services and the global nature of associated risks must be recognised by organisations. As outsourced services are becoming more integrated with organisation's operations, they will have a larger impact on organisation's governance, assurance and control frameworks. It is important to note that risk ownership and accountability remains with agencies and respective risk owners, even when responsibility for specific functions have been outsourced.

5.8.4. Independent assurance reports provide customers and other interested parties with information on policies, procedures and controls related to the service provider's internal frameworks, control objectives and controls in cases where physical inspections and reviews by customers are impractical or not feasible. Service providers may also use the findings of such reports for their own purposes. These reports are used to understand the adequacy and effectiveness of the service provider's frameworks, control objectives, controls and implementation of controls. They allow:

- Business owners to identify and understand the risks associated with the service delivery;
- System owners to more fully assess system risks;
- System designers and security architects to make informed judgements on system structures, controls, defensive measures, and enterprise integration; and
- Regulators, certifiers and accreditors to obtain assurance over the service providers internal control structures and assess the suitability of system structures, controls and defensive measures.

5.8.5. An independent assurance review or third-party audit is invariably undertaken by independent auditors who are not employees of the service provider or their customers. There are two common types of independent third-party reviews: attestation reviews and direct non-attestation reviews.

5.8.6. Attestation reviews, such as an ISAE 3402 review (see below), are generally conducted by accounting or consulting organisations and are based upon recognised attestation standards issued by professional bodies such as the American Institute of Certified Public Accountants (AICPA) or the New Zealand External Reporting Board (XRB).

5.8.7. Direct or non-attestation reviews include those performed by IT consultants or others and may not follow standards referred to previously. They may be based upon other external standards or industry developed criteria such as ISO 2700x, ISACA's COBIT, the IIA, NIST, or the Cloud Security Alliance (CSA).

Assurance

5.8.8. Assurance is derived from an assessment of:

- A description of the service provider's business and control environment;
- Terms and conditions of the service contract or other legally binding agreement;
- Assertions supplied by the service provider (self-assessments);
- An independent validation of service provider assertions;
- Independent testing of controls implementation and effectiveness;

- Assurance in the service design and security architecture; and
- Assurance in the service components.

5.8.9. In general terms, the more ICT services that are outsourced in an agency, the less direct control and visibility the CE and management have over enterprise operations. Therefore, there is an increased reliance on assurance reporting from suppliers. Unless this is recognised in service contracts or legal agreements, agencies may find they are unable to obtain sufficient levels of assurance over the business services and enterprise operations.

Assurance Standards and schemes

ISAE (NZ) 3000

5.8.10. ISAE (NZ) 3000 (Revised) is issued by the External Reporting Board (XRB) of the New Zealand Audit and Assurance Standards Board and is the umbrella standard for other (non-financial) assurance engagements conducted in New Zealand. The standard covers a wide variety of engagements, ranging from assurance on statements about the effectiveness of internal control, for example, to assurance on sustainability reports and possible future engagements addressing integrated reporting. It is a principle-based standard that underpins current and future subject-specific ISAEs (NZ).

ISAE (NZ) 3402

5.8.11. In New Zealand the XRB issued the ISAE (NZ) 3402 in 2014, revised in 2016. This standard has essentially the same requirements as the international standard ISAE 3402 (see below), with some New Zealand specific adaptations. Australia, Singapore and many other jurisdictions have adopted this approach in the issue of this standard with some jurisdiction specific adaptations.

ISAE 3402

5.8.12. The most commonly used international standard for independent assurance reports is the International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization, issued in December 2009 by the International Auditing and Assurance Standards Board (IAASB), part of the International Federation of Accountants (IFAC).

5.8.13. Based on its predecessor standard SAS 70 (1992), ISAE 3402 was developed to provide an international assurance standard for allowing public accountants to issue a report for use by user organisations and their auditors (user auditors) on the controls at a service organisation that are likely to impact or be a part of the user organisation's system of internal control over financial reporting.

5.8.14. Auditing and associated consulting firms were required to use ISAE 3402 for all related work after June 2011.

ISAE 3402 Report Types

5.8.15. The ISAE 3402 provides for a report on controls at a point in time (Type 1 Report) or covering a specified period of time, usually between six and twelve months (Type 2 Report).

5.8.16. A Type 1 report is of limited use as it cannot cover the operating effectiveness of controls and is generally used for new operations where there is no evidence or documented history.

5.8.17. A Type 2 report not only includes the service organisation's description of controls, but also includes detailed testing of the service organisation's controls over a minimum six month period.

5.8.18. It is important to note that the descriptions Type 1 and Type 2 represent an audit approach and should not be confused with SOC 1, 2 and 3 reports under SSAE 16 (see below).

ISAE 3402 Report Uses and Limitations

5.8.19. This standard is used to obtain reasonable assurance about whether:

- The service organisation's description of its system fairly presents the system as designed and implemented throughout a specified period or a specific date;
- The controls related to the control objectives stated in the service organisation's description of its system were suitably designed throughout the specified period or at the specified date;
- Where included in the scope of the engagement, the controls were implemented and operated effectively to provide reasonable assurance that the control objectives stated in the service organisation's description of its system were achieved throughout the specified period.

5.8.20. This ISAE applies only when the service organisation is responsible for, or otherwise able to make an assertion about, the suitable design of controls. It does not cover situations where:

- reporting only whether controls at a service organisation operated as described; or
- reporting on controls at a service organisation other than those related to a service relevant to user entities.

ISAE 3402 Report Content

5.8.21. The ISAE 3402 report usually comprises:

- The service auditor's report;
- Assertions by the service provider;
- A description of control objectives and controls provided by the service organisation;
- Results of any tests and other information provided by the independent auditor; and
- Any other information provided by the service provider.

US Standard SSAE 16

5.8.22. The Statement on Standards for Attestation Engagements No. 16 (SSAE 16) is issued by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). It includes additional requirements to the superseded SAS 70 standard by requiring management to provide a written assertion (see below) regarding the design and operating effectiveness of the controls being reviewed. It is possible that agencies may encounter an SSAE16 based report for a US-based entity.

5.8.23. SSAE 16 is the US equivalent of the international ISAE 3402 and came into effect on 15 June 2011. While the SSAE 16 and ISAE 3402 standards have a common purpose and intent, , there are nine very specific requirements in SSAE 16, not covered in ISAE 3402:

- Intentional acts by the service providers staff;
- Anomalies;
- Direct assistance;
- Subsequent events;
- Statement restricting use of the service auditor's report;
- Disclaimer of Opinion;
- Documentation completion;
- Engagement acceptance and continuance; and
- Elements of the SSAE 16 report that are not required in the ISAE 3402 report.

5.8.24. These differences are summarised in the table below:

	SSAE 16	ISAE 3402
Use of report	Report specifically states it is restricted to intended users.	Report intended for user entities and their auditors but may include other restrictive use conditions.
Intentional Acts	Consideration of the impact of intention acts.	No requirement stated.
Subsequent Events	Auditors must consider Type 2 events after the report date.	Events after the report date are not considered.
Reporting	Sample deviations may not be discarded even when considered non-representative.	Sample deviations are assessed and may be discarded as not representative of the sample population.

5.8.25. The SSAE 16 standard specifies Type 1 and 2 audits (as does ISAE 3402).

5.8.26. A Type 1 is a report on a description of a service organisation's system and the suitability of the design of controls. A Type 1 report will test the design effectiveness of defined controls by examining a sample of one item per control. This provides a basic level of assurance that the organisation has some controls in place. It does not measure the completeness or effectiveness of these controls and represents a point in time.

5.8.27. A Type2 report is a report on policies and procedures placed in operation and tests of operating effectiveness for a specified period of time. A Type 2 report undertakes the tests in a Type 1 report together with an evaluation of the operating effectiveness of the controls for a period of at least six consecutive calendar months.

AICPA Service Organisation Control Reporting (SOC Reports)

5.8.28. Service Organization Control (SOC) Reports, often known as SOC 1, SOC 2, and SOC 3 Reports, are derived from a framework published by the American Institute of Certified Public Accountants (AICPA) for reporting on controls at service organisations.

5.8.29. In New Zealand, SOC 1 reports follow the ISAE (NZ) 3402 standard and SOC 2 reports are follow the ISAE (NZ) 3000 standard, in conjunction with the NZ Standard for Assurance Engagements SAE 3150, for assurance engagements on controls.

5.8.30. Each of the three SOC reports are designed to meet specific needs and reporting requirements for service organisations themselves, rather than being designed to provide assurance to third parties (customers). It is important to note that these reports follow the US (SSAE 16) and Canadian accounting standards, rather than the international ISAE 3402.

SOC 1 Report – Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting. Reporting on controls relevant to internal control over financial reporting and usually conducted in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16 and AT 801 – Reporting on Controls at a Service Organization. A SOC 1 report can be based on a Type 1 or a Type 2 audit.

SOC 2 Report— Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy. SOC 2 Reporting follows the AICPA AT Section 101 (not SSAE 16) and encompasses controls at service organisations on security, availability, processing Integrity, confidentiality and privacy. SOC 2 reports assist in comparing two or more data centres or service providers.

SOC 3 Report— Trust Services Report for Service Organizations. As well as reporting on controls relevant to security, availability, processing integrity, confidentiality and privacy a SOC 3 report provides the same level of assurance about controls over security, availability, processing integrity, confidentiality and/or privacy as a SOC 2 report. The key difference is that a SOC 3 report is intended for general release and does not include the detailed description of the testing performed by the auditor. In place of the detailed description a summary opinion regarding the effectiveness of the controls in place at the data centre or service organisation is provided.

SOC Reports Summary

Report	Standards	Content	Audience
SOC1 – Type 1	ISAE (NZ) 3402/ SAE 3150 or SSAE 16/AT 801	Internal controls over financial reporting at a point in time.	User auditors, organisation finance team, management.
SOC1 – Type 2	ISAE (NZ) 3402/ SAE 3150 or SSAE 16/AT 801	Internal controls over financial reporting over a specified time period, minimum 6 months.	User auditors, organisation finance team, management.
SOC2 – Type 1	ISAE (NZ) 3000/ SAE 3150 or AT 101	Security, availability, processing integrity, confidentiality and privacy controls at a point in time.	Management, regulators, third parties under Non-Disclosure Agreement.
SOC2 – Type 2	ISAE (NZ) 3000/ SAE 3150 or AT 101	Security, availability, processing integrity, confidentiality, privacy controls and operating effectiveness over a specified time period, minimum 6 months.	Management, regulators, third parties under Non-Disclosure Agreement.
SOC3	ISAE (NZ) 3000/ SAE 3150 or AT 101	Security, availability, processing integrity, confidentiality, privacy controls and operating effectiveness.	Public/general use version of SOC 2, excludes details of testing. Is less detailed and has less technical content than a SOC 2 report.

Management Assertions

5.8.31. See Assertions in Certification and Accreditation (NZISM 3.4.3 to 3.4.7) for a short discussion on the nature and purpose of assertions.

5.8.32. The SSAE 16 requires a written assertion by management. Also known as a management's assertion or service organisation assertion it is essentially an assertion made by the service organisation representing and asserting to a number of elements, including:

- The description fairly presents the service organisation's system;
- That the control objectives were suitably designed (SSAE 16 Type 1) and operating effectively (SSAE 16 Type 2) during the dates and/or periods covered by the report; and
- The criteria used for making these assertions, (which are additional statements with supporting matter regarding risk factors relating to control objectives and underlying controls) were in place (Type 1) and were consistently applied (Type 2).

ISO/IEC 27001 Certification

5.8.33. ISO/IEC 27001 is an international standard that provides a framework for Information Security Management Systems. The standard is designed to help organisations of all sizes and types to select suitable and proportionate security controls for information. It provides a structured approach to assist in managing risk by identifying information security vulnerabilities and selecting appropriate controls.

5.8.34. This standard enables independent, external certification bodies to audit the ISMS and certify that the requirements of the standard have been met. Such certification is another means of deriving assurance over the operations of service providers. The requirements for certification are described in the ISO/IEC 27006:2015 standard. Certification is based on two reviews:

- Stage 1 audit (also called Documentation review) checking the systems documentation is compliant with ISO 27001;
- Stage 2 audit (also called Main audit) checking that all the organisation's activities are compliant with both ISO 27001 and the systems documentation.

Other Guidance

Cloud Security Alliance's Security, Trust and Assurance Registry (STAR) Attestation

5.8.35. STAR Certification is a rigorous third party independent assessment of the security of a cloud service provider. It is based on the ISAE 3402 and SSAE 16 standards, supplemented by the criteria in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM).

5.8.36. STAR is a free, publicly accessible registry that documents the security controls provided by various cloud computing service providers. The registry lists three levels of assurance:

1. Self-assessment;
2. Third party assessment based attestation or certification; and
3. Continuous monitoring based certification.

Note: Agencies should note that a self-assessment does not necessarily provide substantive assurance.

5.8.37. As at March 2017, the STAR scheme is still to be fully implemented although there are a number of cloud service providers listed in the registry.

5.8.38. Agencies can use this registry to further inform their judgement on the robustness of assurance over cloud service provider's internal operations and implementation of security controls.

Cloud Security Alliance's Cloud Controls Matric (CCM)

5.8.39. The CCM covers 16 control domains and provides fundamental security principles to guide cloud service providers and to assist prospective cloud customers in assessing the overall security risk of a cloud service provider.

5.8.40. The CCM references and maps its controls to internationally accepted industry standards, regulations, and control frameworks, such as ISO 27001/2/17/18, PCI: DSS v3, and AICPA 2014 Trust Service Principles and Criteria, Germany's BIS, Canada's PIPEDA, ISACA's COBIT, the US FedRAMP, HIPAA, Jericho Forum, NIST and the NZISM.

Cloud Security Alliance's Consensus Assessments Initiative Questionnaire (CAIQ)

5.8.41. The CAIQ is an extension to the CCM that provides exemplar control assertion questions that can be asked of service providers in the context of each CCM control, and can be tailored to suit each unique cloud customer's evidentiary requirements. The Government Chief Digital Officer (GCDO) maintain a mapping of the CAIQ questions to the *GCIO Cloud Security and Privacy Considerations* question set to further aid agencies in use of the CAIQ as an alternative to equivalent GCDO questions.

ISACA IT Audit and Assurance Program for Cloud Computing

5.8.42. Based on ISACA's IT Assurance Framework (ITAF), the Cloud Computing Assurance Program was developed as a comprehensive and good-practice model, aligned with the ISACA COBIT 5 framework. Building on the generic assurance program, the cloud computing guidance identifies a number of cloud specific risk areas encompassing:

- Greater dependency on third parties;
- Increased complexity of compliance with national and international laws and regulations;
- Reliance on the Internet as the primary conduit to the enterprise's data; and
- Risk due to the dynamic nature of cloud computing.

5.8.43. The ITAF assurance focus is on:

- The governance affecting cloud computing;
- The contractual compliance between the service provider and customer;
- Privacy and regulation issues concerning cloud computing; and
- Cloud computing specific attention points.

5.8.44. It is important to note that this cloud computing assurance review is not designed to provide assurance on the design and operational effectiveness of the cloud computing service provider's internal controls, as this assurance is often provided through ISAE 3604 or similar reviews.

5.8.45. The cloud computing assurance review focusses on the agency's or organisation's systems design and operational effectiveness in relation to cloud services. It is also important to note that this is dependent on the effectiveness of the underlying system design and controls and how well these are implemented and managed.

ASD Certified Cloud Services

5.8.46. The Australian Signals Directorate (ASD) conducts certification of cloud services based in Australia for Australian government use. ASD Certifications are based on the Australian Government Information Security Manual (ISM). It is important to note that there are detail differences between the Australian ISM and the NZISM and these documents have a different legislative and regulatory basis.

5.8.47. The ASD Cloud Computing Security documents describe security risk mitigations associated with cloud computing. Australian Government agencies

are also required to perform due diligence reviews of the legal, financial and privacy risks associated with procuring cloud services, aspects which are not covered by the ASD certification.

NIST 800-53

5.8.48. The NIST Special Publication 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations is the US unified information security framework for US federal government agencies. The New Zealand equivalent is the NZISM.

5.8.49. The underlying mandates are in FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems and FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems. US federal government agencies are required to categorise and analyse their system in terms of FIPS 199 and 200 then apply appropriate controls from NIST 800-53.

FedRAMP

5.8.50. The US Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program intended to provide a standardised approach to security assessment, authorisation, and continuous monitoring for cloud products and services. This approach is designed to provide reusable cloud security assessments in order to reduce cost, resource and time. In addition it was intended to minimise cybersecurity risk for Federal Agencies as they move operations to the cloud, provide consistent baseline security policies and streamline the procurement process.

5.8.51. FedRAMP is a collaboration of cybersecurity and cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.

The FedRAMP programme is run by the FedRAMP Program Management Office as part of the GSA.

5.8.52. FedRAMP is mandatory for Federal Agency cloud deployments at all risk impact levels. Private cloud deployments from single agencies and fully implemented within federal facilities are an exception to this mandate. Quarterly reporting by each agency on their cloud portfolio is required.

5.8.53. FedRAMP authorises cloud systems in a three step process:

1. **Security Assessment:** The security assessment process uses a standardised set of requirements in accordance with FISMA using a baseline set of NIST 800-53 controls with additional controls specific to cloud deployments, in order to grant security authorisations. Cryptographic elements are governed by the FIPS 140-2 standards.

2. **Leveraging and Authorisation:** Federal agencies view security authorisation packages in the FedRAMP repository and leverage the security authorisation packages to grant a security authorisation at their own agency.

3. **Ongoing Assessment & Authorisation:** Once an authorisation is granted, ongoing assessment and authorisation activities are required to maintain the security authorisation.

5.8.54. Again it is important to note that the FedRAMP assessments are conducted on a different legislative and regulatory basis to assessments conducted in New Zealand. A variety of guidance, controls, templates and other documentation is available online from the GSA (see References - Assurance Guidance)

PCI DSS

5.8.55. The Payment Card Industry Security Standards Council was formed by major credit card organisations and is a global open body formed to develop and promote understanding of essential security standards for payment account security. It develops, maintains and promotes the Payment Card Industry Data Security Standards (PCI DSS). It also provides tools to assist the implementation of the standards such as assessment and scanning qualifications, self-assessment questionnaires, training and education, and product certification programs.

5.8.56. This standard is designed to protect cardholder data (credit and debit cards) held by merchants, banks and other financial organisations. It applies to all organisations that accept, store, process and transmit credit cardholder data.

5.8.57. This standard is narrowly focussed and has specific applicability to New Zealand Government agencies that operate financial transaction services (e.g. AoG Banking services and citizen fee-paying services; such as vehicle registration, passport renewal, etc.). The PCI has published an information supplement on Third-Party Security Assurance (updated March 2016).

COSO

5.8.58. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) initially developed the COSO Internal Control-Integrated Framework in 1992. A revised framework was published in 2013 which included guidance on “outsourced service providers” and how they impact risk assessment, controls, monitoring, information flows and assurance. The 2013 Framework incorporates how organisations should manage IT innovation in light of globalisation, complex business processes, regulatory demands and security risk assessments. It is frequently used as the basis for SSAE16 assignments and the production of SOC reports.

References – Assurance Standards

5.8.59. Further information on Assurance Standards can be found in:

Reference	Title	Publisher	Source
SSAE No. 16	**Statement on Standards for Attestation Engagements - Reporting on Controls at a Service Organization**	AICPA	https://competency.aicpa.org/media_resources/208710-statement-on-standards-for-attestation-engagements
	Service Organization Controls (SOC) Reports for Service Organizations	AICPA	SOC for Service Organizations: Information for Service Organizations (aicpa.org)
AT Section 101	**Attest Engagements**	AICPA	https://aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-00101.pdf
AT Section 801	**Reporting on Controls at a Service Organization**	AICPA	https://aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-at-00801.pdf
	COBIT 5 Framework	ISACA	https://www.isaca.org/resources/cobit/cobit-5
ISAE (NZ) 3000 (Revised)	**International Standard on Assurance Engagements - Assurance Engagements Other than Audits or Reviews of Historical Financial Information**	XRB	https://xrb.govt.nz/standards/assurance-standards/other-assurance-engagement-standards/
ISAE (NZ) 3402	**International Standard on Assurance Engagements - Assurance Reports on Controls at a Service Organisation**	XRB	https://xrb.govt.nz/standards/assurance-standards/other-assurance-engagement-standards/
SAE 3150	**Standard on Assurance Engagements - Assurance Engagement on Controls**	XRB	https://xrb.govt.nz/standards/assurance-standards/other-assurance-engagement-standards/
NIST Special Publication 800-53 Revision 4	**Security and Privacy Controls for Federal Information Systems and Organizations**	NIST	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [PDF, 5.05 MB]
NIST Special Publication 500-291, Revision 2, July 2013	**NIST Cloud Computing Standards Roadmap**	NIST	https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf [PDF, 2.2 MB]
	PCI DSS Information Supplement: Third-Party Security Assurance	PCI Security Standards Council	https://www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf [PDF, 1.16 MB]
ISO 19011:2018	**Guidelines for auditing management systems**	ISO	ISO - ISO 19011:2018 - Guidelines for auditing management systems
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 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 security, cybersecurity and privacy protection — Guidelines for information security management systems auditing**	ISO	https://www.iso.org/standard/77802.html
ISO/IEC TS 27008:2019	**Information technology — Security techniques — Guidelines for the assessment of information security controls**	ISO	https://www.iso.org/standard/67397.html
ISO/IEC 27014:2020	**Information security, cybersecurity and privacy protection — Governance of information security**	ISO	https://www.iso.org/standard/74046.html
ISO/IEC 27017:2015	**Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services**	ISO	https://www.iso.org/standard/43757.html
ISO/IEC 27018:2019	**Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors**	ISO	https://www.iso.org/standard/76559.html

References – Assurance Guidance

5.8.60.

Reference	Title	Publisher	Source
	All-Of-Government Portfolio, Programme and Project Assurance Framework	DIA	https://digital.govt.nz/standards-and-guidance/governance/system-assurance/all-of-government-portfolio-programme-and-project-assurance-framework/
	All-Of-Government ICT Operations Assurance Framework	DIA	https://digital.govt.nz/standards-and-guidance/governance/system-assurance/all-of-government-ict-operations-assurance-framework/
	All-Of-Government Enterprise Risk Maturity Assessment Framework (gERMAF)	DIA	https://digital.govt.nz/standards-and-guidance/governance/system-assurance/enterprise-risk-maturity/
	FAQs — New Service Organization Standards and Implementation Guidance	American Institute of Certified Public Accountants (AICPA)	https://docplayer.net/13378742-Faqs-new-service-organization-standards-and-implementation-guidance.html
	The Federal Risk and Authorization Management Program (FedRAMP)	General Services Administration, US Federal Government	https://www.fedramp.gov/
	FedRAMP Documents & Templates	General Services Administration, US Federal Government	https://www.fedramp.gov/documents-templates/
	Controls and Assurance in the Cloud Using COBIT 5	ISACA	Store - Controls & Assurance in the Cloud: Using COBIT 5	Digital	English - ISACA Portal
	IIA Position Paper: THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL JANUARY 2013	IIA	121691 PROF-Position Paper 3 Lines of Defense_Digital Version_CK.indd (theiia.fi)

Rationale & Controls

Risk Assessment

5.8.61.R.01. **Rationale**

The Security Risk Management Plan (SRMP – Section 5.3) encompasses all risks associated with the security of agency systems. The growth in outsourced services, particularly cloud services, has created situations where risk, controls and assurance cannot be directly examined and assessed. In such cases independent assurance reports are an effective means, possibly the only means, of obtaining some assurance on the service provider's operations.

5.8.61.R.02. **Rationale**

No single independent assurance scheme/standard covers the full range of considerations and control requirements of the NZISM. Agencies may find duplication of aspects analysed if multiple schemes are applied. It is also important to note that none of the common mature assurance schemes cover specific government requirements and handling of Official Information; such as the personnel aspects (PERSEC) of user and administration vetting and security clearances, or sovereignty aspects of the information/data. Careful selection and consideration is required when placing reliance on reports available for a particular outsourced or cloud service.

5.8.61.R.03. **Rationale**

Reports from different assurance scheme have varying levels of detail as well as risk area coverage. Selection and usage of reports should be considered in the context of the intended service/system business and information value.

Understanding the business and technical risk context will drive the size and depth of a risk assessment, and the associated assurance process. Though even a lighter-weight risk assurance process will follow the C&A process model, such that the CE or authorised delegate is still formally accountable and responsible.

Re-use of assessments completed by other agencies is encouraged, noting the business or information value context may differ. To assist agencies and promote efficiency, the Government Chief Digital Officer (GCDO) facilitates the sharing and re-use of existing cloud assessment materials among agencies.

5.8.61.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1019]

Agencies MUST conduct a risk assessment in order to determine the type and level of independent assurance required to satisfy certification and accreditation requirements.

5.8.61.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1020]

In all cases where assurance on service provider operations cannot be obtained directly, agencies SHOULD obtain independent assurance reports.

5.8.61.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1021]

In order to address identified risk areas, agencies SHOULD obtain relevant assurance reports and service provider certifications to inform a risk assessment and Certification activities as well as other aspects of the certification processes such as evidence of controls effectiveness and remediation plans.

Independent Assurance

5.8.62.R.01. **Rationale**

Independent assurance can be obtained directly from the service provider through Service Organisation Control (SOC) reports, as well as other internationally recognised assurance frameworks. It will be important to corroborate individual reports by comparison with other reporting mechanisms and independent certifications.

5.8.62.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1024]

Agencies MUST incorporate the results of any independent assurance reports into the agency Certification process, to understand the residual risk position and controls required to manage risk appropriately.