Frequently asked questions and answers
Attestation under the NSW Government Digital Information Security Policy

OFS, May 2014
informationsecurity@finance.nsw.gov.au

1. Does my agency need to attest?

The NSW Government Digital Information Security Policy (the Policy) is issued under a Premier’s Memorandum. Agencies subject to Premier’s Memoranda, including statutory bodies, that produce an annual report containing the agency's financial report will need to attest.

This includes all entities that produce annual reports in line with the Annual Reports (Statutory Bodies) Act 1984 and the Annual Reports (Departments) Act 1985.

Copies of past annual reports should be available on your agency’s website. They will include an introduction from the head of the agency, or other text, stating which Annual Reports Act the report complies with.

If your agency does not produce an annual report containing your agency's financial report, please determine which organisation's annual report your agency is covered by and make contact with the Senior Responsible Office (SRO) who is responsible for information security at that agency.

Note: Your communications and marketing team, or agency head’s office will be able to help answer questions about annual reports. If you need to coordinate with another agency, you can find a list of SRO contact details on govdex.

2. What are Secretaries / CEOs attesting to?

They are attesting to compliance with the Policy, including that:

- they had an Information Security Management System (ISMS) during the reported financial year, that is consistent with the Core Requirements of the Policy
- taking into account business requirements of the agency, adequate security controls are in place to mitigate identified risks to digital information and systems for the foreseeable future
- all public sector agencies under the control of the agency, with a risk profile sufficient to warrant an independent ISMS, have developed an ISMS in accordance with the Policy, and
- where applicable, certified compliance with ISO/IEC 27001 by an accredited third party has been obtained and maintained.
3. I'm not sure whether my agency can attest. What should I do?

If your agency has met the requirements of the Policy, attest in your annual report, without qualification.

If you have any concerns about meeting the requirements of the Policy, then attest to your current state of compliance. In this scenario you are attesting as to what you have achieved, in terms of the maturity of your ISMS, the Security Categories in the Policy, and the relevant ISO 27001 controls.

You should use the existing attestation template and you may need to modify the wording according to your agency’s particular circumstances to ensure the statement accurately reflects your current situation. You should draft your attestation so as not to allow information security vulnerabilities to be incorrectly inferred from its wording.

Any modifications should cover:
- what your agency has done towards achieving compliance with the Policy
- any areas that require additional focus, and
- your agency’s forward plan.

You can also:

a) Discuss attestation with the CIO to ensure s/he is across the requirements of attestation and what the attestation template means.

b) Liaise with your “parent agency” and with the SRO from that agency, including the cluster representative on the Information Security Steering Group, to determine how the attestation and agency ISMS fits in with the “parent agency” attestation and ISMS.

c) Refine the scope of the ISMS, and obtain certification in relation to the appropriate part of the agency’s information system.

d) Liaise with the shared service provider, because in many cases you may find that the shared service provider’s ISMS and attestation already covers a significant part of your agency’s information system.

e) Apply a maturity model approach to attestation and include wording around the attestation in the annual report explaining how this has been applied in the agency’s circumstances.

f) Brief the senior executive in relation to any significant difficulties with meeting the Policy requirements, including attestation.

g) Liaise with your agency Audit and Risk Committee, if appropriate.

If you require further assistance, please contact the Information team at OFS via email at informationsecurity@finance.nsw.gov.au
CLASSIFICATION AND LABELLING

4. In order to attest, do I need to have implemented a classification and labelling system that is consistent with the Commonwealth system?

Controls in the Policy require agencies to have a system of information classification in place (controls 7.2.1, 7.2.2, ISO 27001). This is relevant to attestation.

The Policy also requires implementation of an approach to classification and labelling that is consistent with the Commonwealth scheme. However, agencies are not required to have achieved this consistency in order to report that they have a system of information classification in place.

Agencies that have not yet implemented a system consistent with the Commonwealth approach are still able to attest. If your agency has any concerns about the maturity of the information classification program then you can add words such as the following to your attestation:

“The transition to an information classification and labelling scheme as required by the Policy is in progress. The planned completion date is [x].”

5. In relation to classification and labelling, does my agency need to have adopted every part of the Commonwealth Protective Security Policy Framework (PSPF)?

No. The Policy requires implementation of an approach to classification and labelling that is consistent with the Commonwealth scheme.

The classification and labelling requirements in the Policy and NSW Government Information Classification and Labelling Guidelines (the Guidelines) apply to information classified or labelled after 1 January 2014 – and only to sensitive information.

You only need to comply with the Guidelines, which set out a modified Commonwealth approach, tailored to NSW Government requirements. Where it is necessary to apply elements of the PSPF it is recommended that agencies take a pragmatic approach.

HOW TO ATTEST

6. Do I need to include all four paragraphs of the attestation template as set out in the Policy?

You should include an attestation as per the template. This template has been drafted so that paragraphs that do not necessarily apply in an agency’s particular circumstances can still remain in the attestation.

If you are unable to include all four paragraphs, you should include as much of the text from the attestation template as you can. You may modify the wording to the extent necessary to accurately reflect your agency’s particular circumstances.
7. I am from a shared service provider. Can I attest for the entities which my organisation provides shared services to?

No. Shared service providers are not responsible for the attestation of entities to which they provide services.

8. Whose name should appear in the attestation text?

The name of the agency head (Secretary, CEO, Director or other) should be included in the attestation text.

9. In the attestation text, what is meant by ‘Public Sector Agencies under the control of the Department or Statutory Body’?

An agency ‘controls’ a sub-agency when it has the capacity to dominate the decision-making, financial and operational, of that sub-agency. The sub-agencies under the control of the parent agency should be listed in the parent agency’s annual report.

ANNUAL REPORTS

10. Does the ISMS need to have been in place for the entire year that the annual report covers?

No. The ISMS may have already been in existence prior to the commencement of the relevant financial year, or established during that year.

11. My agency does not produce an annual report. Does this mean it is exempt from attestations?

If your agency is not required to produce an annual report in accordance with the Annual Reports Act, it is not your agency’s responsibility to attest. Your agency will be covered by another agency’s annual report and should be mentioned in its foreword or other text explaining which agencies it covers.

If you would like to contact SROs from the agency that your annual reporting is covered by, you can find these contact details on govdex.

12. Where are annual reports published?

It is a legal requirement that annual reports for Government agencies must be:

- made available to the public on the agency’s website, and
- presented to Parliament and made available for publishing on Parliament’s website.

You can find out more about NSW legislation for annual reports.
BACKGROUND ON ATTESTATION

13. What is attestation under the Policy and why do agencies need to attest?

Attestations in annual reports are a requirement of the Policy, starting with the 2013-14 financial year. Standard text is used to express that the agency is complying with minimum information security controls.

The Policy helps enhance information security across all NSW public sector agencies and shared service providers, by mandating the development of an ISMS and compliance with international best practice standards, including ISO 27001.

Ongoing attestations support the focus of the Policy on the development of an ISMS that ensures information security is an ongoing risk management process.

Annual reports are submitted to the Minister, the Treasurer and Parliament.

Annual attestation also provides citizens of NSW with confidence that government agencies are adhering to best practice policy and standards for managing and protecting the State’s information assets.

14. What is an Information Security Management System (ISMS)?

An ISMS is an organisational approach that involves identifying information security risks and putting security controls in place to manage them. Taking a risk-based approach, the ISMS should be documented and should include the minimum controls drawn from ISO 27001 as set out in the Policy.

15. How do I know if my agency is fully compliant with the minimum controls in the Policy?

Attestation does not require perfect or fully mature compliance with each of the Security Categories or controls in the Policy. The attestation requires that information security is well managed and that controls in place are ‘adequate for the foreseeable future’. It is recommended that agencies adopt a maturity model approach to attestation.

Some SROs have found that involving their Audit and Risk Committee and legal counsel in reviewing their position helps them gain confidence in their attestation. Your colleagues in Audit and Risk or Legal may be able to provide a paragraph or two to help explain your position for the briefing to the head of your agency.

16. Does attestation equate to being confident that there will be no security breaches?

The nature of information security means there are no guarantees that security breaches won’t happen. This is why we use a risk-based approach for information security and put in place plans to address risk progressively in the future.

17. I am still unsure about attestation.

No problem. Please contact the Information team at OFS via email informationsecurity@finance.nsw.gov.au for assistance.