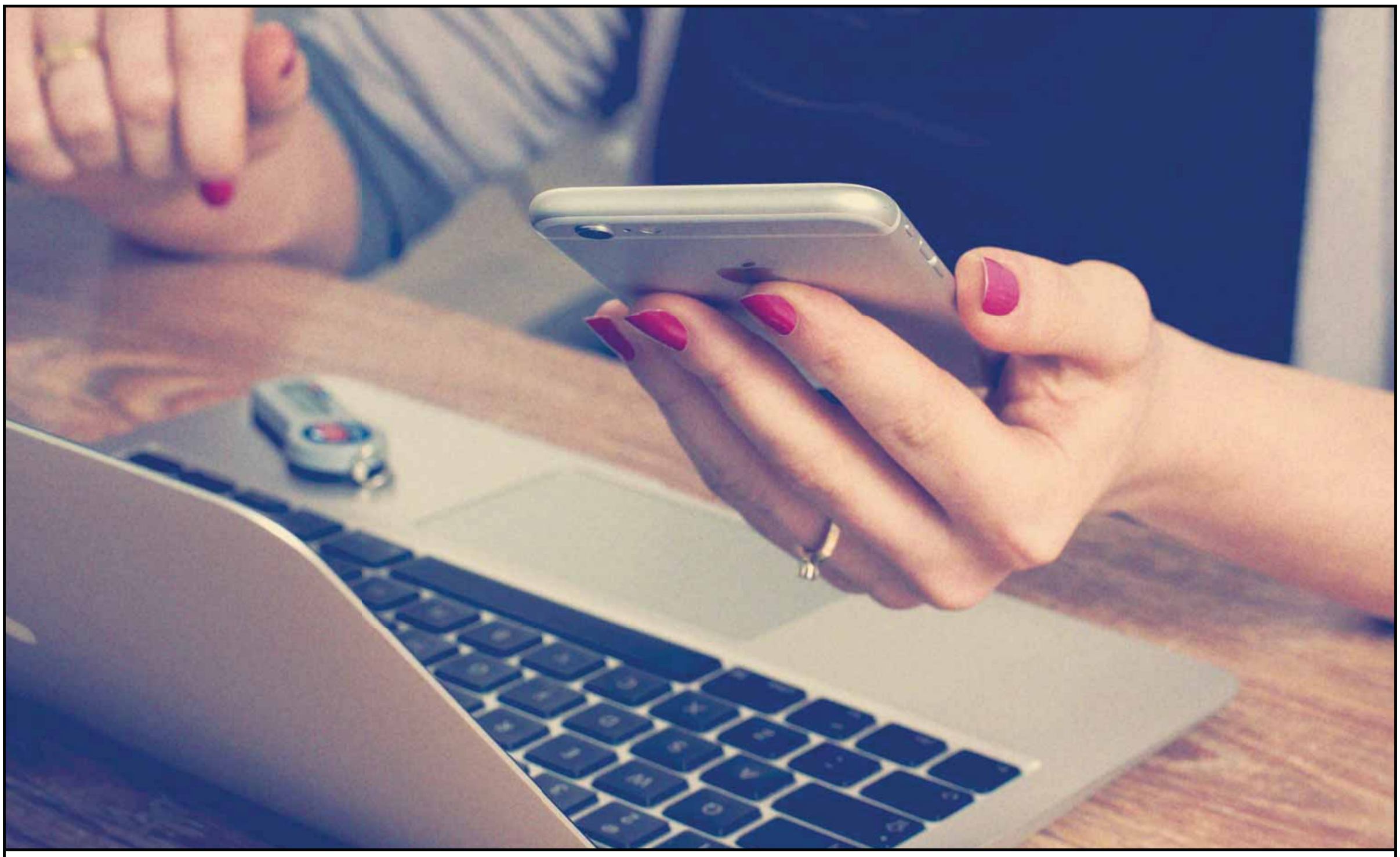


CERTIFICATION & ACCREDITATION GUIDE

Governing and protecting our systems.

02

MadeCurious.

Contents

Welcome

Background

Definitions

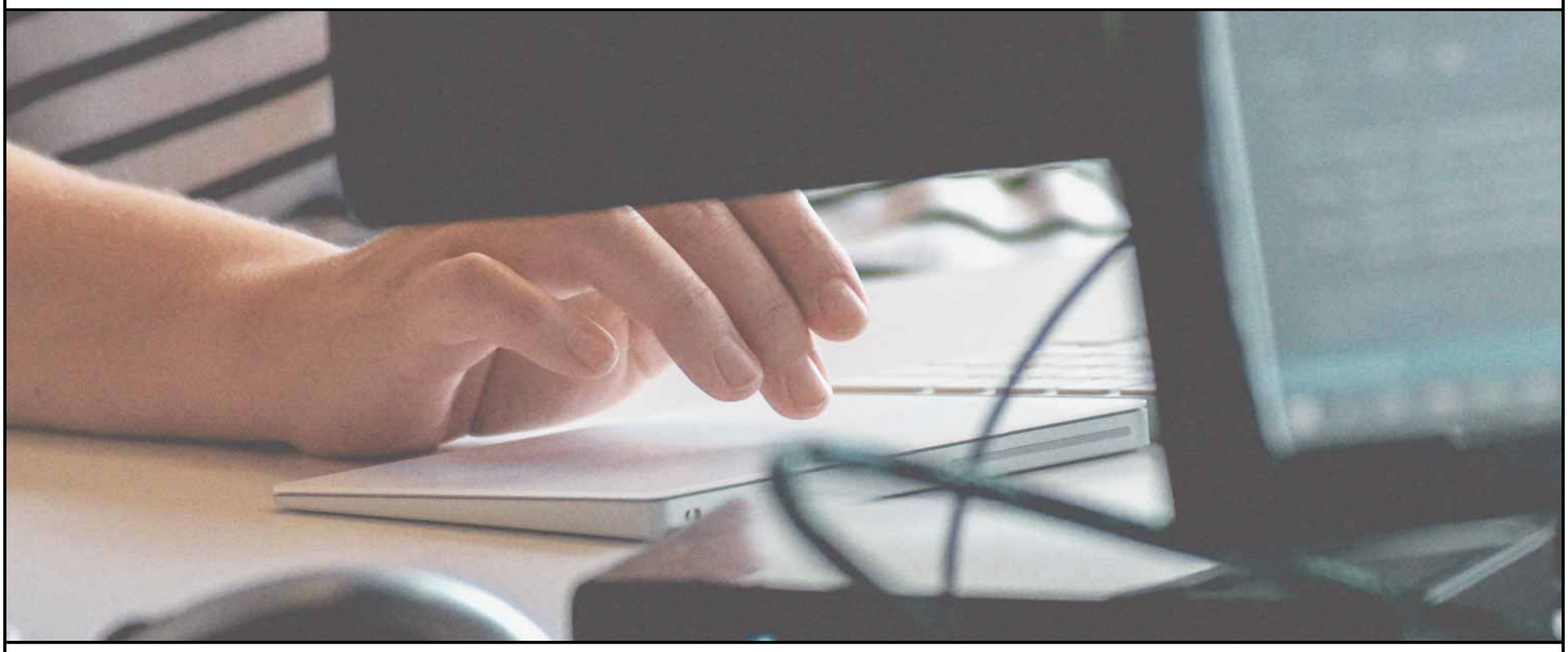
C&A Overview

Certification Stages

Accreditation Stages

Managing the product owner - vendor relationship

Summary



Welcome

Security and governance is an essential part of providing ICT services and systems for government, and awareness around its importance is rapidly growing.

That's why we've developed this guide to Certification and Accreditation (C&A) for public sector departments and their product owners. We've combined our experience and knowledge gleaned from working with experts and PO's from leading agencies to give you a detailed walkthrough of the C&A process from both points of view - the department's and the vendor's.

Some agencies are championing its use as part of an All-of Government Uplift programme to maintain the excellence of the public sector's digital security going into the future.

While C&A is mandated and has been around for a while, there is a current push to mature the process. If you haven't started on the C&A journey and you work in (or for) a public sector agency, it is very likely that you will soon.

Who this guide is for

Certification & Accreditation can be a joint effort between product owners and managers, internal security teams, third party security contractors, and the ICT vendors who develop the product requiring certification. If you fit into any of these roles, this guide is for you.

Note: There may be other third parties involved on short engagements, such as penetration testing service providers.

Background

Certification and Accreditation is a fundamental governance and assurance process, designed to provide the Board, Chief Executive and senior executives of government agencies confidence that:

- Information and its associated technology are well-managed
- Risks are properly identified and mitigated
- Governance responsibilities can demonstrably be met

It is essential for credible and effective information assurance governance:

- Certification must always take place before accreditation. Both are separate and distinct elements that contribute to good governance.
- In both stages, decisions are based on an assessment of risk, the application of controls described in the The New Zealand Information Security Manual (NZISM), and determination of any residual risk. Certification must be completed before accreditation can take place.
- The acceptance of residual risk lies with the Chief Executive of each agency, or lead agency where sector, multi-agency or All-of-Government (AoG) systems are implemented.

Definitions

Certification is evidence that due consideration has been paid to risk, security, functionality, and business requirements.

It is the assertion that a given ICT system (product) aligns with minimum standards and the agreed design. It is based on a comprehensive evaluation to confirm the system has been appropriately audited, remediated or controlled to meet desired standards.

Once certified, and if applicable to your agency, your digital product is issued with a Service Security Certificate (SSC). This might not be the process for every product, especially those that are not an AoG product or system.

Accreditation is the formal authority to operate a system. Accreditation is given based on evidence that governance requirements have been addressed and that the Chief Executive has fulfilled the requirement to manage risk on behalf of the organisation and stakeholders.

C&A Overview - Phases & Stages

NB. Some agencies will be moving to continuous certification and for those that do, the processes will differ slightly.

PHASE 1: Certification & Assurance

Certification is required before accreditation can be granted.

To achieve certification:

1. Identify that no current security certificate exists (it may have recently expired) and start the process to gain certification
2. Conduct a certification audit and report on the requirements for meeting best practice
3. Implement your recommended controls and remediations to meet best practice
4. Conduct a validation audit to report the fixes of issues found in the original audit

The relevant authority assesses your reported residual risk position when deciding to grant certification. Certification can be granted for one, two, or three
year durations.

Assurance

Once certification is granted, annual assurance plans and activities may be required to validate the security position of the product to maintain certification.

For each year of your certification:

1. Conduct an annual assurance plan reporting on remediation actions for the maintenance of best practice standards
2. Provide evidence of meeting best practice standards

When certification expires, you need to begin the process from the start.

PHASE 2: Accreditation

Accreditation concerns reporting the product's risk position (created by certification) and demonstrates that approval has been provided for the use of the system by senior stakeholders. It is essentially rubber stamping that enough has been done to create a risk position that is acceptable and there is confidence that this position will be maintained.

In summary Phase 1 is all about gaining certification and assuring it while Phase 2 is all about gaining official approval (accreditation) to operate the system in its current state. Certification demonstrates that particular standards have been met, assured that they can be maintained and Accreditation accepts the risk position and approves use.

4 Key Stages of C&A

01

Certification

No current security certificate identified - start the process to gain certification. Conduct audits, reviews and create reports to understand what needs to be done to reach the desired security standards. Conduct recommended controls and remediation. Conduct a final audit to report on the residual risk position and present for certification. If certification is unsuccessful, you may be asked to remediate and establish extra controls.

02

Accreditation

Accreditation is the official approval to operate. Evidence produced in the certification process is presented, including the annual assurance plan, and instils enough confidence that security best standards have been met and will be maintained.

03

Certificate Maintenance

Certification can vary in length. Assurance Plan’s are executed to ensure the risk position (or score) is maintained with an annual plan of varying activities for each year of the current certification, i.e. a 3 year certificate means 3 cycles of the assurance plan/ activities. Reporting on the progress of remediation is part of the assurance plan.

04

Recertification

When the certification expires you go back to the start (step 1) and proceed through the process again.

Phase 1

Stage 1: Certification

The product owner identifies or is made aware that a product does not have a certificate or the current certificate is due to expire, and therefore must begin planning to rectify. A product owner will need to engage with multiple stakeholders to organise the kick-off for the C&A process.

Content Audit

Who: Product owner, the security team (external and internal) and the product vendor
Objectives: A Certification Audit assesses the actual implementation and effectiveness of controls or remediation for a system against the agency's:

- Risk profile
- Security posture
- Design specifications
- Agency policies
- Compliance with the Protective Security Requirements (PSR).

Early in the Certification Audit, recommendations will be made on what remediation and controls should be applied to the system to achieve standards. The audit is then repeated after the recommended remediation and controls have been actioned to measure the

resulting risk. This resulting, or residual risk, is evaluated and depending on the risk appetite, will be accepted or recommend further action.

Note: The extent and scope of the Certification Audit is dictated by the feasibility and cost-effectiveness of the audit against the risks and benefits of the system under review. Major or high-risk systems will require more detailed and extensive review than low-risk or minor systems.

Phase 1

Assurance plan

Once you have gained certification, begin planning to conduct annual assurance plans. The Product Assurance Plan instils checkpoints to ensure obligations are being met and maps out the accreditation activities staggered at different times of the year (some are annual, monthly, quarterly or bi-annually).

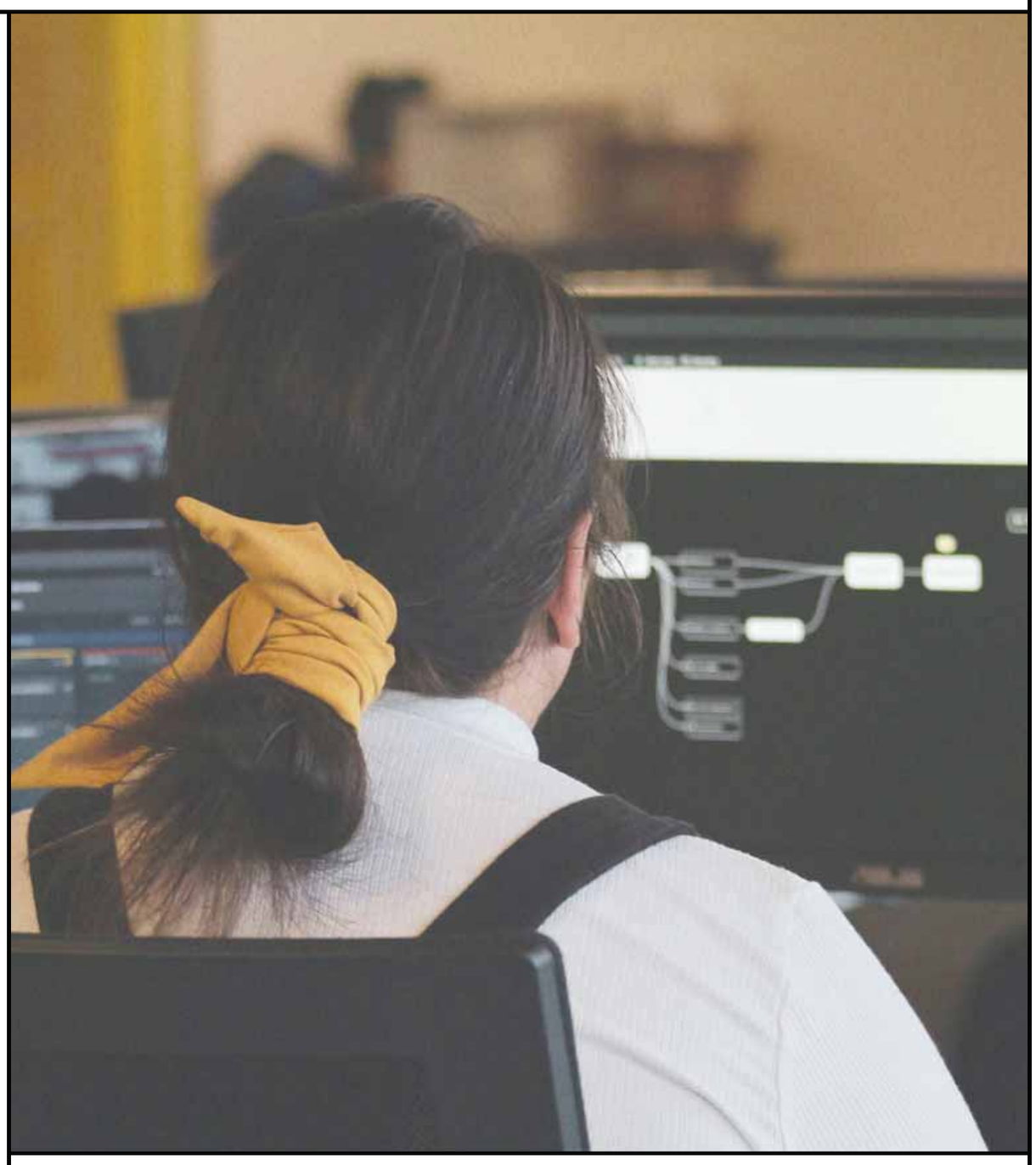
Who: Product owner, vendor and internal security team
The activities detailed in your assurance plan:

- Are specific to the product and its risk position
- Take place throughout each calendar year of your certification to provide assurance evidence

Objectives:

- Develop a framework that ensures that accreditation activities are conducted in a repeatable and consistent manner across the agency and that consistency across government systems is maintained. This is a fundamental part of a robust governance model and provides a sound process to demonstrate good governance of information systems. Assurance plans can be the most demanding part of C&A, however, having a clear plan will help immensely with understanding the requirements, executing them and measuring performance.
- Place checkpoints to ensure obligations are being met as part of accreditation activities staggered at different times of the year (annual, monthly, quarterly or bi-annually). Ongoing assurance maintains certification of the service and ensures that the system's security posture is maintained within the window it is certified.

Tip! Share the assurance plan early (it doesn't need to be complete or perfect) with your product vendor. It can be a great tool for communicating the important steps and timescales to help them plan and prepare resources to support you.



Example Assurance Plan activities

Activities will vary according to the type of system and its function, as too will the frequency of said activities.

- Penetration Testing
- Operational Security Reviews
- Code Reviews
- DR & BCP Testing
- Firewall Reviews & Host Reviews
- Vulnerability Scans
- Patch and Vulnerability Management Review
- Backup Testing
- Access Management Review

Phase 1

Audit Activities:

Produce the following key documents to complete a certification audit:

1 **Security Design Review & Threats Assessments Report**
Who: The security team (external or internal) conducts a security design review to compare the product with industry best practice.

Objectives:

- Security Design Review: Identify any security flaws in the proposed design before the audit activities commence

Threat Assessment Report: Examine the security threats specific to the product and identify the potential disruption or damage

2 **Product Risk Assessment Report**
Who: The security team (external or internal) conducts an information security risk assessment for the use and operation of the product and compiles their findings in this report.

Objectives:

- Find and categorise risks on a risk position index which visualises and prioritises each risk according to the stated risk appetite.
- Report on the expected residual risk position if all recommended security controls and remediations are implemented and appropriately managed. It considers the business risk in terms of data, privacy, stakeholders, integrity, business impact, confidentiality and security risk.

The risk assessment generally has a Gross Risk Score(a view of risk without controls) and a Residual (target) Risk Score (with all the controls).

These scores are very useful because they provide a view or marker of the best and worst case scenario.

3 **Control Validation Plan & Audit**
Who: The security team (external or internal) develops a plan for a control validation audit (CVA) before conducting the audit itself.

Objectives:

- Control Validation Plan:
  - Define the audit methodology for the CVA
  - Detail the risks and controls identified in the Product Risk Assessment Report alongside corresponding controls to be used during the audit
- Control Validation Audit: Validate that key security controls have been implemented and operate effectively

4 **Remediation Register**
Who: The product owner and vendor or service owner work together to build a register of all recommended remediations and their current statuses, whether scheduled, completed or pending.
Objective: Provide updates on remediation and controls

Certification Granted

Certification is issued if the above documents (evidence) included in the certification audit demonstrate due consideration to risk, security, functionality, and business requirements.

Who: Product owner and Certification Authority
Objective: Officially recognise that the risk position is in alignment with the Agency's risk appetite
Certification has been issued because acceptable evidence has been provided to demonstrate that due consideration has been paid to:

- Risk
- Security
- Functionality
- Business requirements

Phase 2

Accreditation Gained

Who: Product owner and the Agency CISO
Objective: Accreditation declares information is protected and measures are in place and active to maintain that position.

Accreditation is issued when the product owner demonstrates that either:

- Sufficient security measures have been put in place to protect information processed, stored or communicated by the system

or

- Deficiencies in such measures have been identified, assessed, and acknowledged - including the acceptance of any residual risk

Once Accreditation is achieved, product owners need to repeat assurance plans for each year of the certificate to maintain it. For example, if your product has been given a three-year certificate, you must conduct an annual assurance plan three years in a row.

We call this the Assurance Phase which provides evidence and assurance that you are doing everything possible to monitor and maintain security standards for the system.

Tip! Do not submit your assurance plan for accreditation until all relevant certifications have been provided. The Accreditation Authority for a specific system can never accredit a system until that happens.

Vendor perspective

Choose vendors who are set up to cater for the demands of the C&A process. Pulling together all the required activities can take a sizable coordination effort for both product owners and vendors. As a vendor, we work with the product owner to provide different types of evidence such as:

- security policies
- evidence of testing
- logs and alerts
- DR/BCP plans
- back-up procedures
- risk register

These are just some of the types of evidence your vendor will need to provide during audits.

Phase 2

Managing the product owner - vendor relationship

A good relationship between product owners and vendors is crucial for completing the demands of the C&A process. It pays for both parties to be organised. But building trust is also essential, to strengthen communications and resource management.
As a vendor, we advise product owners to:

Communicate information early
The more information and process you can share, the more your vendor can prepare evidence and plan remediation.

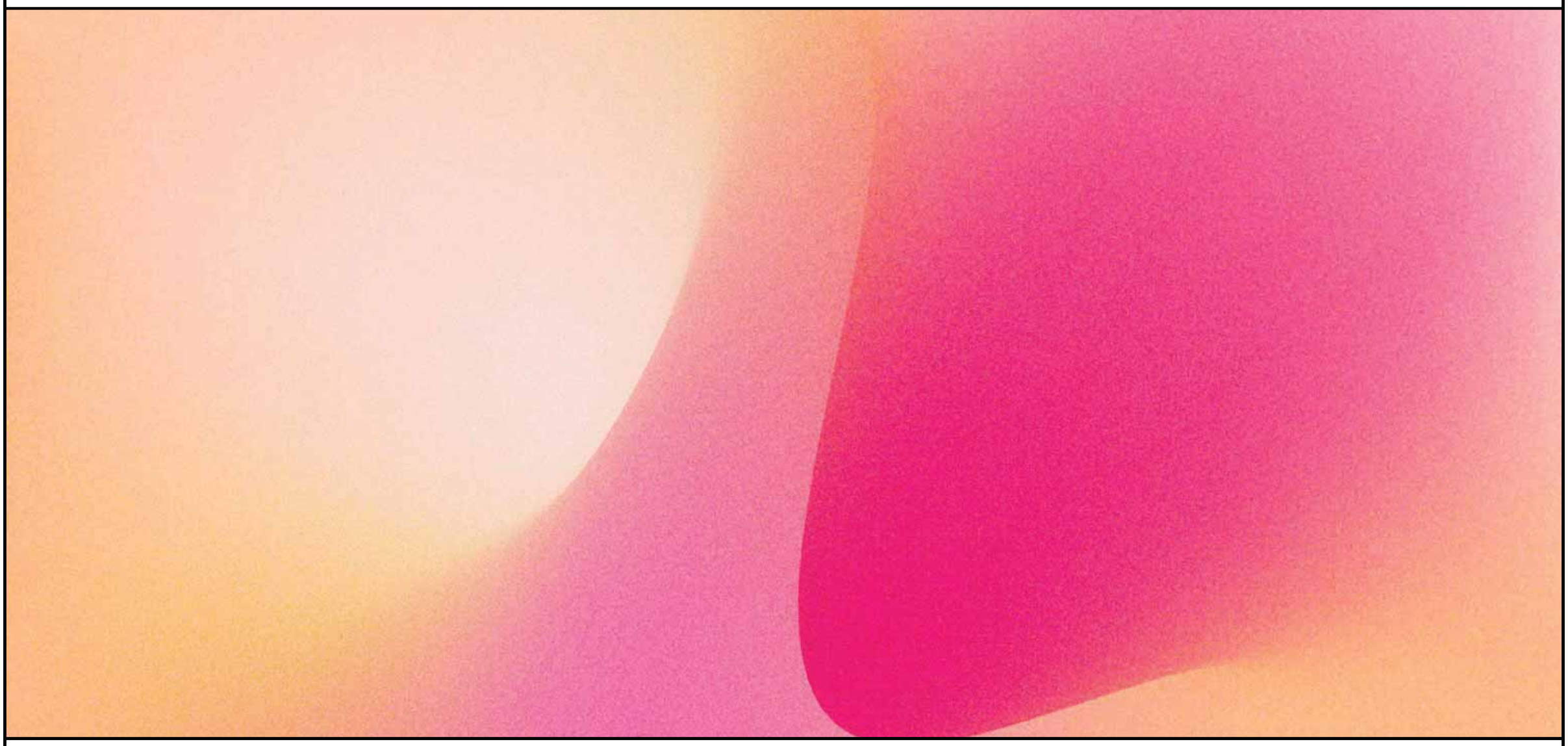
Take your vendor on a journey
If your vendor has no or little experience in this process, spend some time building their understanding.
Identify your stakeholders before you startBring them together at the start to share plans and concerns, and build rapport.

Put remediation at the top of every to-do list
As you move through identifying risk and remediation, keep shuffling this to the top of the deck and communicate it with your vendor early and often. This gives the vendor more opportunity to plan and prepare for remediation.

You don’t have to be perfect!
If there is too much to do, prioritise what is most important and action it. For less important remediations you can use letters of intent to assure it will be done and therefore not creating risk of failure to gain accreditation.

Ask third-party security contractors to consider other vendors time carefully
They need to consider the time commitments of other vendors when scheduling long audit meetings and make sure they group all the parts needed for vendors together, so they only need to attend the parts relevant to them.

Make sure your Vendor understands the timeframes well and feels comfortable meeting them
If there are problems meeting timeframes, work with your vendor to plan alternatives that are communicated to the auditors. If there are problems meeting timeframes in the first year, consider how you could better prepare the vendor for the following year. For example, by providing more notice.



Summary

It may seem daunting at first, especially if this is the first time you are moving through the C&A process.

Not every agency or product will need to comply to the same level. The importance of products vary based on the type of service or data it provides, the different risk profiles, and the level of acceptable tolerance.

The trend observed overseas is to increase compliance. It is an important demonstration of a government's commitment to the security of their systems, data, and services. If you’re not invested yet, you very likely will need to be.

PHONE
+64 3 365 2887

EMAIL
hello@madecurious.com

WEBSITE
madecurious.com