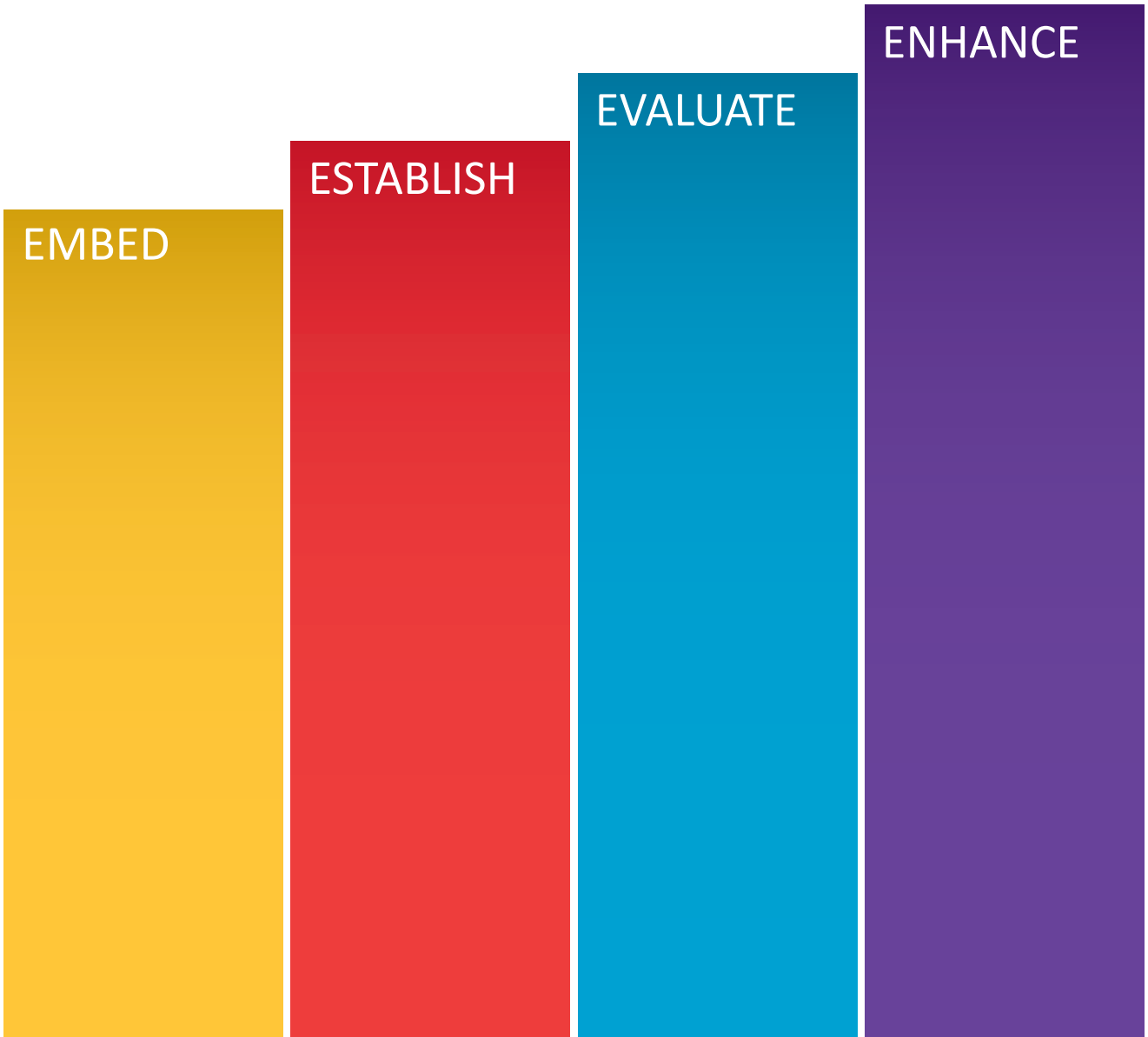
Australian Government

Office of the Australian Information Commissioner

Privacy management framework:

enabling compliance and encouraging good practice



INTRODUCTION

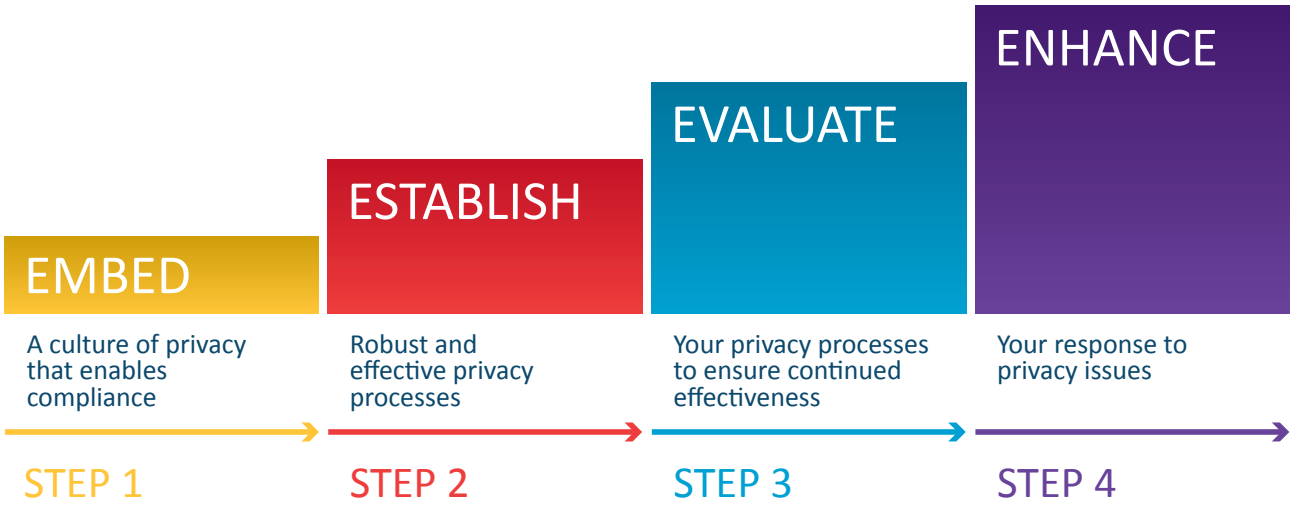
This *Privacy management framework* (Framework) provides steps the Office of the Australian Information Commissioner (OAIC) expects you to take to meet your ongoing compliance obligations under Australian Privacy Principle (APP) 1.2.

APP 1 ensures that personal information is managed in an open and transparent way. APP 1.2 requires you to take reasonable steps to implement practices, procedures and systems that ensure compliance with the APPs. This means that you must be proactive in establishing, implementing and maintaining privacy processes. Compliance with APP 1.2 should be understood as a matter of good governance.

A leadership commitment to a culture of privacy is a foundation for good privacy governance. Good privacy governance can improve business productivity and help to develop more efficient business processes. Good privacy governance will also help you manage both the risk of a privacy breach and your response should one occur.

Personal information is one of your most valuable business assets. By embedding a culture that respects privacy, you will build a reputation for strong and effective privacy management that will inspire trust and confidence in your entity.

The Framework has four steps. These are the steps you should take to ensure you practice good privacy governance and meet your ongoing compliance obligations. Which commitments you implement within each step, and who performs these, will depend upon your particular circumstances, including your entity's size, resources and business model.



STEP 1: EMBED

A culture of privacy that enables compliance

Good privacy management stems from good privacy governance. Ensure your leadership and governance arrangements create a culture of privacy that values personal information.

To embed a culture of privacy, make a commitment to:

- treat personal information as a valuable business asset to be respected, managed and protected. Outline how protecting personal information is important for your business
- appoint key roles and responsibilities for privacy management, including a senior member of staff with overall accountability for privacy. Also have staff responsible for managing privacy, including a key privacy officer, who are responsible for handling internal and external privacy enquiries, complaints, and access and correction requests
- adopt a 'privacy by design' approach. Ensure you consider the seven foundational principles of privacy by design in all your business projects and decisions that involve personal information
- allocate resources to support the development and implementation of a privacy management plan that aligns your business processes with your privacy obligations. Your plan should outline how you will implement and monitor the steps outlined in this Framework, and meet your goals or objectives for managing privacy
- implement reporting mechanisms that ensure senior management are routinely informed about privacy issues
- understand your privacy obligations. The *APP guidelines* provide guidance on how the OAIC will interpret the APPs and what matters it may take into account when exercising its functions and powers
- understand the role of the OAIC. The *Privacy regulatory action policy* explains the OAIC's approach to using its privacy regulatory powers and how it will communicate information.

STEP 2: ESTABLISH

Robust and effective privacy practices, procedures and systems

Good privacy management requires the development and implementation of robust and effective practices, procedures and systems.

To establish good privacy practices, procedures and systems, make a commitment to:

- keep information about your business's personal information holdings (including the type of information you hold and where it is held) up to date. This includes information held off-shore, or that is in the physical possession of a third party
- develop and maintain processes to ensure you're handling personal information in accordance with your privacy obligations. Ensure these processes:
  - address the handling of information throughout the information lifecycle — prior to collection, once personal information has been collected, while you hold it and once it is no longer needed. Ensure additional consideration is given to areas you assess as having greater risk, including sensitive information and use of service providers, contractors, outsourcing arrangements and off shore storage
  - clearly outline how staff are expected to handle personal information in their everyday duties. Tailor these processes to align with the different needs of different parts of your business, and how they use personal information
- promote privacy awareness within your entity by integrating privacy into your induction and regular staff training programs (including short term staff, service providers and contractors). This should include training staff on their privacy obligations and your processes. The OAIC has a number of training resources to help you with this
- develop and implement a clearly expressed and up to date privacy policy. Ensure your privacy notices are also up to date and consistent with your privacy policy. The *Guide to developing an APP privacy policy* provides tips and a checklist to help you develop and assess your privacy policy
- implement risk management processes that allow you to identify, assess and manage privacy risks across your business, including personal information security risks. The *Guide to securing personal information* provides steps and strategies you should consider taking to protect personal information, including privacy impact assessments, information security risk assessments and regular reviews of your personal information security controls
- undertake privacy impact assessments for business projects or decisions that involve new or changed personal information handling practices (including implementing new technologies). The *Guide to undertaking privacy impact assessments* includes information on threshold assessments, which will help you determine whether a privacy impact assessment is necessary
- establish processes for receiving and responding to privacy enquiries and complaints. The *Handling privacy complaints* resource provides information to help you address a privacy complaint
- establish processes that allow individuals to promptly and easily access and correct their personal information
- develop a data breach response plan. The *Data breach notification — A guide to handling personal information security breaches* provides guidance to assist you respond effectively to data breaches.

STEP 3: EVALUATE

Your privacy practices, procedures and systems to ensure continued effectiveness

Systematically examine the effectiveness and appropriateness of your privacy practices, procedures and systems to ensure they remain effective and appropriate.

To evaluate your privacy practices, procedures and systems, make a commitment to:

- monitor and review your privacy processes regularly. This could include assessing the adequacy and currency of your practices, procedures and systems, including your privacy policy and privacy notices, to ensure they are up to date and being adhered to
- document your compliance with your privacy obligations, including keeping records on privacy process reviews, breaches and complaints. Ensure senior management and those with responsibility for privacy management are briefed on risks or issues identified
- measure your performance against your privacy management plan. Regularly review your implementation of this Framework and your progress towards your objectives or goals
- create channels for both your staff and customers to provide feedback on your privacy processes, such as a suggestion box and feedback form.

STEP 4: ENHANCE

Your response to privacy issues

Good privacy management requires you to be proactive, forward thinking and to anticipate future challenges. By continually improving your privacy processes, you will ensure you are responsive to new privacy issues and that implementation will not be a burden.

To enhance your response to privacy issues, make a commitment to:

- use the results of your Step 3 evaluations to make changes to your practices, procedures and systems that improve your privacy processes. Track the performance of any new measures you implement
- consider having your privacy processes externally assessed to identify areas for improvement
- consider adopting good privacy practices that go beyond the requirements of the APPs, where appropriate. The *APP guidelines* and other OAIC resources provide examples of good privacy practices
- keep informed of issues and developments in privacy law and changing legal obligations. Subscribe to the OAIC's news email list OAICnet for updates and participate in privacy seminars, including the OAIC's webinars
- monitor and address new security risks and threats. Subscribe to Stay Smart Online Alert Service and follow the steps it suggests for ensuring online security, including implementing software updates and patches. The Australian Cyber Security Centre and CERT Australia provide guidance on cyber security issues
- examine and address the privacy implications, risks and benefits of new technologies. Consider implementing privacy enhancing technologies that allow you to minimise and better manage the personal information you handle
- introduce initiatives that promote good privacy standards in your business practices. Highlight examples of good personal information handling so that your staff know what is expected of them
- participate in Privacy Awareness Week and other privacy events. By bringing privacy into the spotlight, you will ensure your staff remain privacy aware.

Office of the Australian Information Commissioner

GPO Box 5218 Sydney NSW 2001
enquiries line: 1300 363 992
email: enquiries@oaic.gov.au

www.oaic.gov.au