Australian Government
Office of the Australian Information Commissioner

Privacy and Registered Training Organisations

Lessons from an OAIC privacy assessment

Brett Watson, Assistant Director, Regulation and Strategy, OAIC

Kerry Hutchinson, General Manager - Quality and Compliance, Navitas

7 August 2018

OAIC

In today’s webinar:

1. About the OAIC and our privacy assessments
2. The RTO survey assessment
   a) Positive findings
   b) Areas for improvement
3. Navitas – lessons learned
4. Tips for good privacy practice
5. Q and A

About the OAIC

About the OAIC

- Privacy, freedom of information, information policy
- Far-reaching jurisdiction and diverse stakeholders
- A variety of regulatory functions and powers to promote privacy and enforce the Australian Privacy Principles (APPs)
- oaic.gov.au
- 1300 363 992

The legal framework

- RTOs are regulated by overlapping laws and regulations
- *Privacy Act 1988* (Cth)
- Various state and territory privacy laws apply to state and territory government agencies
- *Student Identifiers Act 2014* (Cth)

Privacy assessments (audits)

- A proactive measure
- Public and private sectors
- Flexible methodologies depending on the objective and scope
- oaic.gov.au/privacy-law/assessments/

Australian Government

Office of the Australian Information Commissioner

The RTO survey assessment

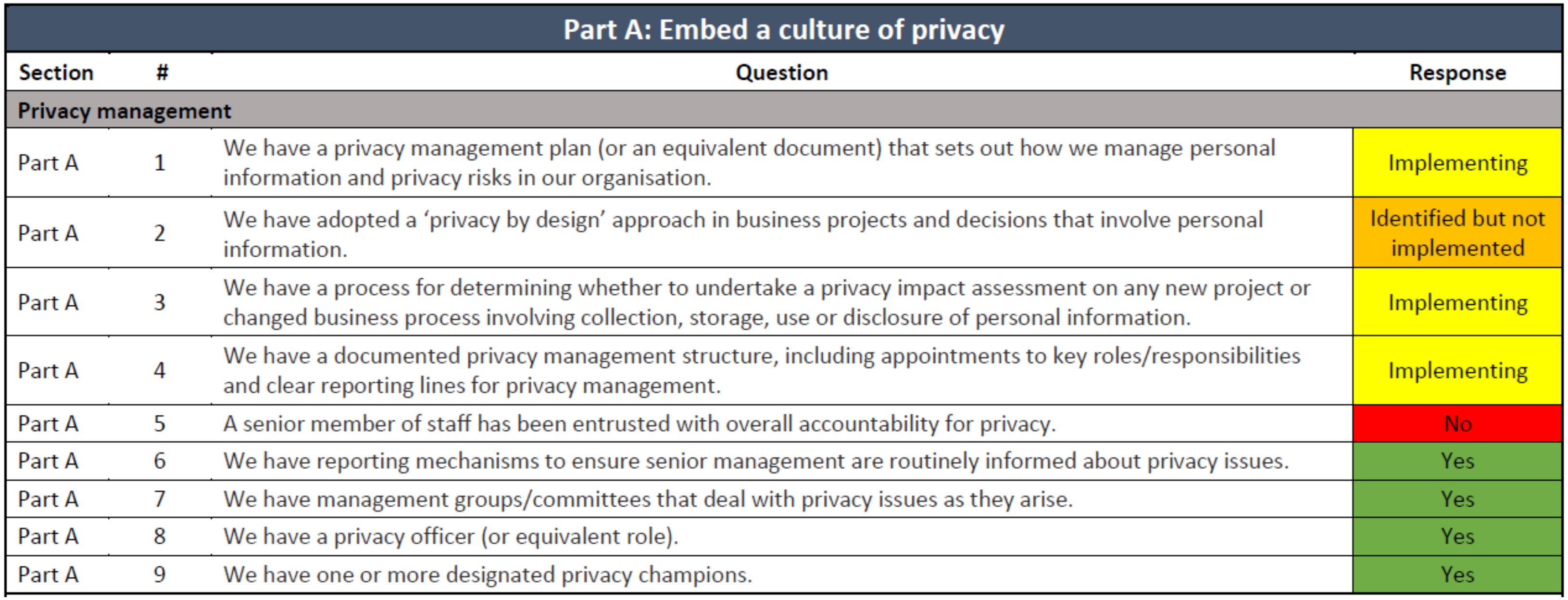
OAIC

Scope

- APP 1
  - open and transparent management of personal information
  - APP privacy policy
- APP 5
  - notification of the collection of personal information

Methodology

- Agreed between the OAIC and the USI Office
- Selected five RTOs based on certain criteria
- Conducted via a self-administered smart form survey in November 2017



Part A: Embed a culture of privacy

Section	#	Question	Response
Privacy management			
Part A	1	We have a privacy management plan (or an equivalent document) that sets out how we manage personal information and privacy risks in our organisation.	Implementing
Part A	2	We have adopted a 'privacy by design' approach in business projects and decisions that involve personal information.	Identified but not implemented
Part A	3	We have a process for determining whether to undertake a privacy impact assessment on any new project or changed business process involving collection, storage, use or disclosure of personal information.	Implementing
Part A	4	We have a documented privacy management structure, including appointments to key roles/responsibilities and clear reporting lines for privacy management.	Implementing
Part A	5	A senior member of staff has been entrusted with overall accountability for privacy.	No
Part A	6	We have reporting mechanisms to ensure senior management are routinely informed about privacy issues.	Yes
Part A	7	We have management groups/committees that deal with privacy issues as they arise.	Yes
Part A	8	We have a privacy officer (or equivalent role).	Yes
Part A	9	We have one or more designated privacy champions.	Yes

Australian Government

Office of the Australian Information Commissioner

Navitas - participating in the privacy assessment

OAIC

Navitas Limited – the Audit landscape

- The audit process involved Navitas English Pty Ltd, a member of the Navitas Limited Group
- Increased data security and privacy regulation
- The audit coincided with Navitas Limited’s review of:
  - Global policies and procedures
  - Information security environment and IT architecture
  - Managing information, personal and commercial

Navitas Limited – the Audit process

- The OAIC is a key resource
- Protecting privacy and data sovereignty is a global phenomenon
- Getting to know another Regulatory Authority
- Objective, external perspective on our privacy management systems, processes and policies
- Breadth and depth of privacy management – holistic governance approach needed
- Embedding the Privacy Principles as standard ‘good practice’ is essential

Navitas Limited – key imperatives

- Enhance awareness and understanding of privacy principles
- Operationalise privacy principles – everyone is responsible for protecting privacy
- Embed ‘privacy by design’ into Company culture
- Standardise and regularise training for all staff
- Implement awareness of and need for Privacy Impact Assessment (PIA)
- Train staff – administrative and academic

Australian Government

Office of the Australian Information Commissioner

Assessment results

OAIC

Positive findings

- Clear processes for collecting and disclosing personal information
- Processes to ensure data quality
- Enabling students to access and correct their personal information
- Effective complaint handling mechanisms

Areas for improvement

- Privacy practices that move from operations up to the governance level
- Privacy training for new and existing staff
- Having privacy policies and collection notices available in alternative languages and formats

Areas for improvement

- Data breach response
- Information security
  - Policy reviews
  - Access monitoring

Australian Government

Office of the Australian Information Commissioner

Navitas – Lessons learned

Navitas Limited – What did the Audit change?

- Privacy fundamental to Company culture
- Global commitment to Privacy by Design (PxD) across all operational activity
- Privacy management and acceptance of APPs built into terms and conditions of employment
- Implementing the GDPR across all operating regions
- Privacy Management is not a ‘silo’ activity - it’s a global responsibility
- Getting it wrong is a costly business!

Navitas Limited – What's happening now?

- Developed and implemented Data Subject Access Request (DSAR) Procedure
- Established, implemented and tested Data Breach Management procedure – triage approach
- Implemented global privacy management platform
- Implemented compulsory staff training - managing personal information; reporting suspected breaches
- Privacy framework, policy and procedure revitalised in line with APPs and GDPR requirements

Navitas Limited – What’s happening now?

- Established global network of Data Protection Managers (DPM’s) in each operating region and global community of practice (CoP)
- PxD workshops developed and being implemented
- Privacy Notice translated into seven languages with more to come
- Revised approach to consent; complaints; accessing personal information
- PIA and DPIA embedded into Project and new initiatives design and development

Australian Government

Office of the Australian Information Commissioner

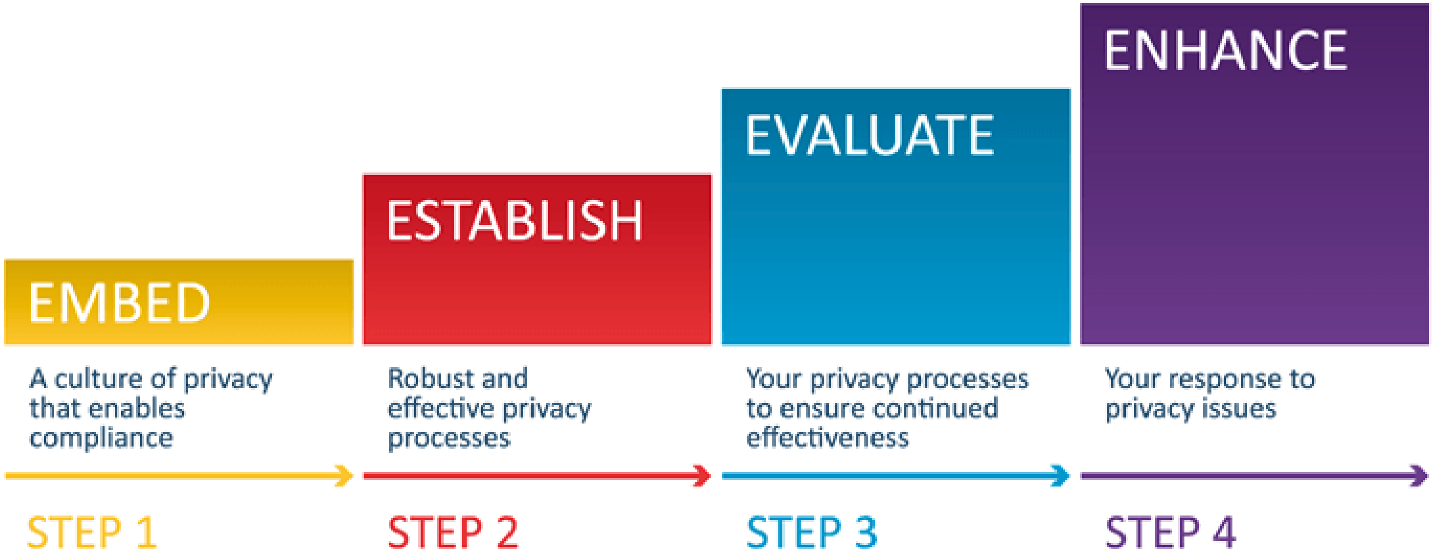
Tips for good privacy practice

OAIC

Privacy governance

- Appoint a ‘privacy champion’ amongst your senior leadership group
- Privacy management plans (PMPs) are a good way to document your approach to privacy governance
- PIAs can feed into PMPs
- Privacy Management Framework on our website

Privacy governance



EMBED

A culture of privacy that enables compliance

STEP 1

ESTABLISH

Robust and effective privacy processes

STEP 2

EVALUATE

Your privacy processes to ensure continued effectiveness

STEP 3

ENHANCE

Your response to privacy issues

STEP 4

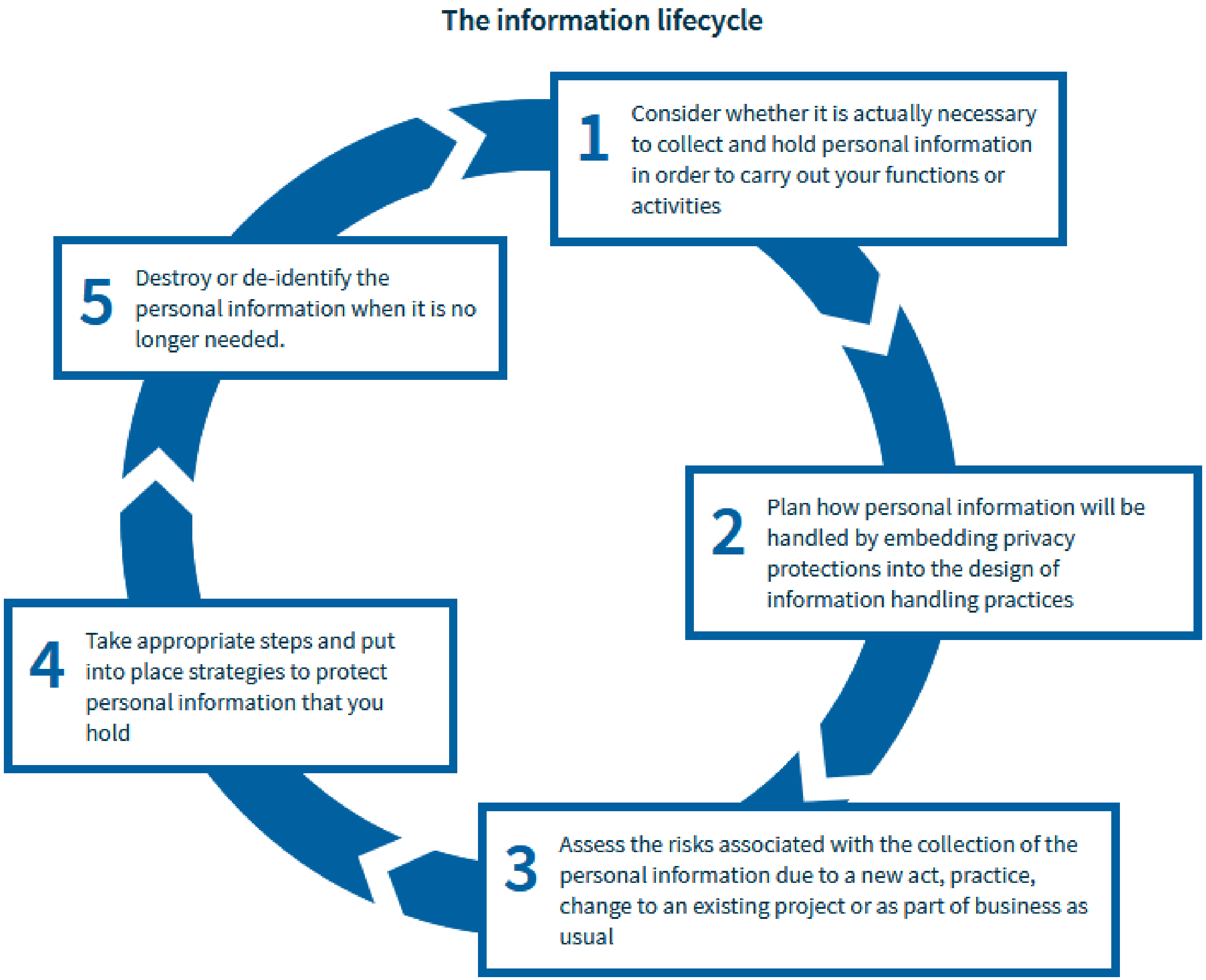
Privacy training

- For all staff: full time, part time, temporary and contractors
- Upon commencement and refreshed as necessary
- Reduce the potential for human error
- https://www.oaic.gov.au/agencies-and-organisations/training-resources/

Data breach response

- NDB scheme effective since 22 February 2018
- New notification obligations
- OAIC resources for agencies and organisations available online
- https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

Personal information security



The information lifecycle

1 Consider whether it is actually necessary to collect and hold personal information in order to carry out your functions or activities

2 Plan how personal information will be handled by embedding privacy protections into the design of information handling practices

3 Assess the risks associated with the collection of the personal information due to a new act, practice, change to an existing project or as part of business as usual

4 Take appropriate steps and put into place strategies to protect personal information that you hold

5 Destroy or de-identify the personal information when it is no longer needed.

Q and A

Links to resources:

- Privacy Management Framework:

  https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework

- Guide to securing personal information:

  https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information oaic.gov.au