Meeting PROV Compliance requirements
Security Management

6th October 2017

Toula Varvarigos

PO Box 1370 Fitzroy North
Victoria 3068 Australia 1300 804 254
www.eassure.com.au
contact@eassure.com.au

Outcomes

Training Outcomes

- Develop an understanding of PROV's records security requirements.
- Develop an understanding of the definition of information security vs security management for records,
- Identify current drivers for information security including legislative obligations.
- Identify the business context for information security.
- Understand why information security is important.
- Understand information security components
- Identify information security risk and governance requirements.
- Develop principles and Key Performance Indicators (KPI) for information security
- Understand information security monitoring and compliance reporting.

Information Security – the players

DTF

- The Victorian Information Security policy and standards were developed by DTF and released in late 2012.
- The standards require inner WoVG agencies to develop their own information security management framework (ISMF), which is to be based on the policy and standards. This includes annual reporting requirements on the status of information security within the agency, and an assessment of its ability to withstand a cyber attack.
- These new policy and standards apply to only 20 agencies and were communicated through the following key documents: SEC POL 01: Information Security Management Policy, SEC STD 01: Information Security Management Framework and SEC STD 02: Critical Information Infrastructure Risk Management.

https://www.audit.vic.gov.au/sites/default/files/20131127-WoVG-Info-Security.pdf

https://www.enterprisesolutions.vic.gov.au/wp-content/uploads/2016/02/SEC-STD-01-Information-Security-Management-Framework.pdf

Information Commissioner (OVIC)

- The new commissioner will oversee the current Victorian privacy and law enforcement data security regimes and will implement a Victorian Protective Security Policy Framework, across the Victorian public sector.

Information Security – the players

OVIC - continued

- A public sector body Head for an agency or body to which this Part applies must ensure that a contracted service provider of the agency or body does not do an act or engage in a practice that contravenes a protective data security standard in respect of public sector data collected, held, used, managed, disclosed or transferred by the contracted service provider for the agency or body. (PDPA PART FOUR, SECTION 88 part 2)
- Require contracted service providers with direct or indirect access to information to adhere to the standards. (section 16)
- To ensure the protection of public sector data across the core security domains, through the appropriate inclusion of the VPDSS in any contracted service provider arrangements.
- Protocol 9.1 Prior to the engagement of contracted service providers, the VPDSS are considered in the planning, development and scoping of the security requirements in the organisation's contracted service provider arrangements.
- Protocol 9.2 Security requirements are embedded in the organisation's contracted service provider arrangements.
- Protocol 9.3 Security requirements are appropriately monitored and reviewed in the organisation's contracted service provider arrangements.
- Protocol 9.4 Security requirements are improved and the organisation's contracted service provider arrangements are updated to respond to the evolving security risk environment.
- https://www.cpdp.vic.gov.au/images/content/pdf/data_security/20160721%20VPDSS%20Control%20reference%20links%20V1.0.pdf

PROV's compliance requirements

Security Management
Procedures are developed and all staff members (including volunteers and contractors) who are authorised to make changes to records are instructed in how to add, delete/remove, or alter records and capture these changes appropriately.. Capture PROS 11/07, Specification 3, Section 2.5, Requirement 14.
Records that carry security classifications are created and captured in compliance with the requirements of that classification. Capture PROS 11/07, Specification 3, Section 2.5, Requirement 17
A security policy for records is established and communicated to all relevant members of staff, including contractors and volunteers. PROS 11/10: Access Specification 1: Access to Records in Agency Custody, section 2.5, Security, requirement 13.
Security measures, procedures and protocols relating to access to records are established, documented, and designed to prevent unauthorised access, alteration, destruction or release. PROS 11/10: Access Specification 1: Access to Records in Agency Custody, section 2.5, Security, requirement 14
Record security obligations are communicated to all members of staff, including contractors and volunteers , and training provided. PROS 11/10: Access Specification 1: Access to Records in Agency Custody, section 2.5, Security, requirement 15.
The recordkeeping audit programme includes monitoring, assessment and reporting on the security of records. PROS 11/10: Access Specification 1: Access to Records in Agency Custody, section 2.5, Security, requirement 16.

To begin……What is Information Security?

Definition Search

Information Management

The way in which an organisation plans, identifies, creates, receives, collects, organises, governs, secures, uses, controls, disseminates, exchanges, maintains, preserves and disposes of its information. It is also the means through which the organisation ensures that the value of that information is identified and used to its full potential.

Information Security

A risk management process designed to safeguard official information assets and services in a way that is proportionate to threats and supportive of business. It uses a combination of procedural, physical, personnel, information and ICT security measures designed to provide government (organisations) information, functions, resources, employees and clients with protection against security threats. Also referred to as data protection or information security.

https://www.cpdp.vic.gov.au/images/content/pdf/data_security/20160628_VPDSF_Glossary_of_Protective_Data_Security_Terms_V1.0.pdf

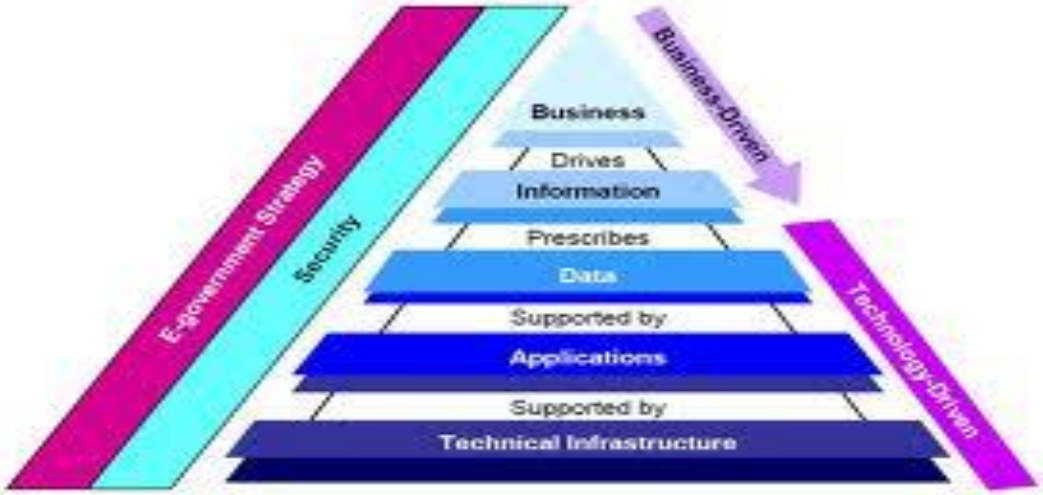
A Common Understanding… IM

Information Definition

A common understanding

Unstructured: These are records (information) comprised of word documents, emails, memos, web content and is usually of a text format or combination of text, images and other formats. Unstructured information can reside in a number of places, including file servers, web servers, personal computers and in electronic document and records management systems and business applications.

Structured: This is the data (information)on contained in business applications systems and includes financial, human resources, client and planning data. It is typically captured and stored in database table format; profiles and organised such that it can be easily identified, retrieved and re-used.



eassure INFORMATION INNOVATION

What is data?

- Facts or instructions represented in a formalised manner, suitable for transmission, interpretation or processing manually or automatically.

Adapted from: International Council on Archives, Dictionary of Archival Terminology, KG Saur, Munich, 1988, p. 48.

Don’t forget Metadata

- Metadata summarizes basic information about data, which can make finding and working with particular instances of data easier.
- For example, author, date created and date modified and file size are examples of very basic document metadata.
- Having the ability to filter through that metadata makes it much easier for someone to locate a specific document.
- In addition to document files, metadata is used for images, videos, spreadsheets and web pages.
- Metadata can be created manually, or by automated information processing. Manual creation tends to be more accurate, allowing the user to input any information they feel is relevant or needed to help describe the file. Automated metadata creation can be much more elementary, usually only displaying information such as file size, file extension, when the file was created and who created the file.

What is a record?

Record

- A record is all information created, sent and received in the course of carrying out the business of your agency. Records have many formats, including paper and electronic. Records provide proof of what happened, when it happened and who made decisions. Not all records are of equal importance or need to be kept.

AS-ISO 15489, Part 1, Clause 3.15.

Babushka Doll – Information Management…..to apply Information Security

Data Metadata Record Information

eassure INFORMATION INNOVATION

Brainstorm 1: Why is records security important to your organisation? (15 minutes)

Why is it important?

- The security of records is essential to ensuring their reliability, integrity and evidential value.
- All the organisation's systems, workplaces and storage areas that contain official records are designed and managed to protect them from unauthorised access, alteration or deletion, and staff are aware of and follow the procedures to ensure this.
- Security classifications for records are known by all staff and are assigned to all records at the time of creation or receipt in line with the degree of protection the information in the record requires.
- A security classification/level is assigned to all staff by the respective business unit managers and is appropriate to the staff member's need to know the information in the record in order to conduct legitimate business for the organisation.
- The organisation has procedures in place to review and declassify official records that are classified 'In-Confidence' and above at an appropriate time if protection is no longer necessary or is no longer needed at the original level.
- The organisation assigns responsibility for monitoring access to, alteration and movement of official records, using audit logs within the corporate records management system and business systems containing records.
- Avoid the embarrassment, financial costs and legal implications of unauthorised access to official records.
- Reduction in the costs associated with locating hard to find records.
- Easy access to the records required to deliver agency business, leading to better customer service.
- Minimise the chances for illegal alteration to or illegal disposal of official records.
- Increased confidence in the reliability and evidential value of official records required to support and authenticate the actions and decisions of an agency.

Brainstorm 2: What do you need to do in order to meet the requirements? (15 minutes)

What do you need to meet the requirements?

https://www.parliament.vic.gov.au/publications/research-papers/download/36-research-papers/13824-protective-data-security-in-the-victorian-public-sector

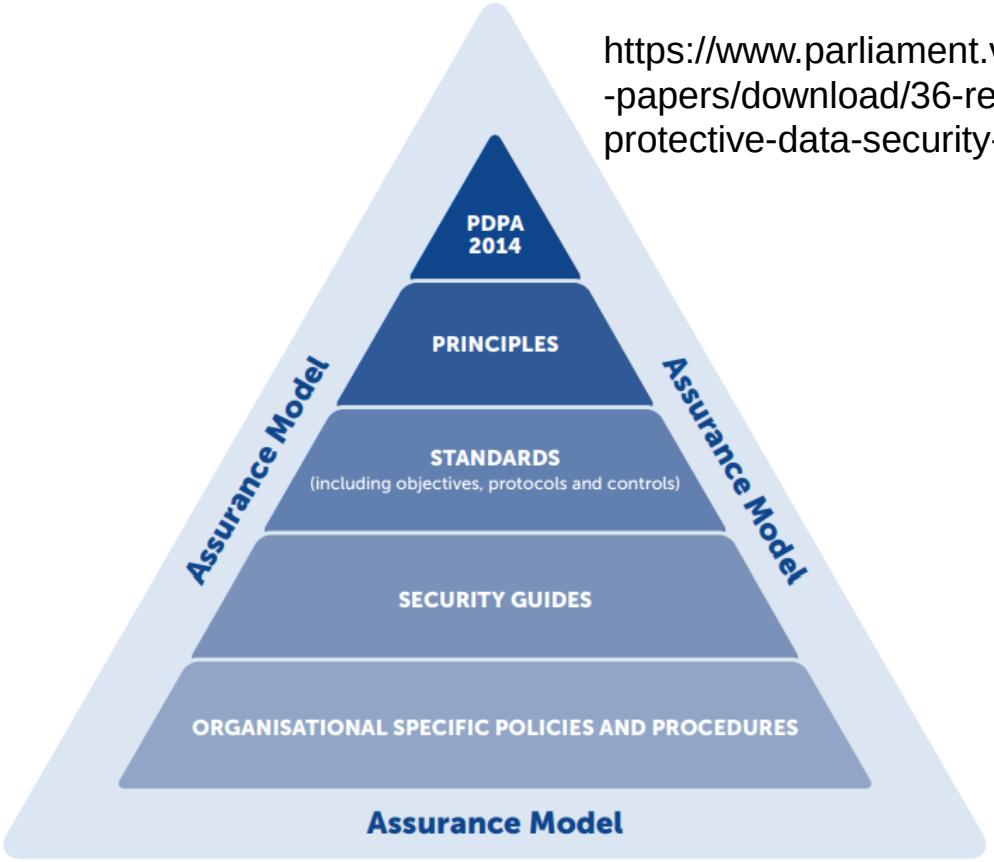


Figure 1. VPDSF structure

eassure INFORMATION INNOVATION

It depends on what your responsible for ?

	Information Management	Records Management
Security Management Framework *(Security governance)*	An organisation must establish, implement and maintain a security management framework proportionate to their size, resources and risk posture.	
Security Risk Management *(Security governance)*	An organisation must utilise a risk management framework to manage security risks.	
Security Policies and Procedures *(Security governance)*	An organisation must establish, implement and maintain security policies and procedures proportionate to their size, resources and risk posture.	
Information Access *(Security governance)*	An organisation must establish, implement and maintain an access management regime for access to public sector data.	
Security Obligations *(Security governance)*	An organisation must define, document, communicate and regularly review the security obligations of all persons with access to public sector data.	

It depends on what your responsible for ?

	Information Management	Records Management
Security Training and Awareness *(Security governance)*	An organisation must ensure all persons with access to public sector data undertake security training and awareness.	
Security Incident Management *(Security governance)*	An organisation must establish, implement and maintain a security incident management regime proportionate to their size, resources and risk posture.	
Business Continuity Management *(Security governance)*	An organisation must establish, implement and maintain a business continuity management program that addresses the security of public sector data.	
Contracted Service Providers *(Security governance)*	An organisation must ensure that contracted service providers with access to public sector data, do not do an act or engage in a practice that contravenes the VPDSS.	
Government Services *(Security governance)*	An organisation that receives a government service from another organisation must ensure that the service complies with the VPDSS in respect to public sector data that is collected, held, used, managed, disclosed or transferred.	
Security Plans *(Security governance)*	An organisation must establish, implement and maintain a protective data security plan to manage their security risks.	
Compliance *(Security governance)*	An organisation must perform an annual assessment of their implementation of the VPDSS and report their level of compliance to the Victorian Information Commissioner.	

It depends on what your responsible for ?

	Information Management	Records Management
Information Value *(Information security)*	An organisation must conduct an information assessment considering the potential compromise to the confidentiality, integrity and availability of public sector data.	
Information Management *(Information security)*	An organisation must establish, implement and maintain information security controls in their information management framework.	
Information Sharing *(Information security)*	An organisation must ensure that security controls are applied when sharing public sector data.	
Personnel Lifecycle *(Personnel security)*	An organisation must establish, implement and maintain personnel security controls in their personnel management regime.	
Information Communications Technology (ICT) Lifecycle *(ICT security)*	An organisation must establish, implement and maintain Information Communications Technology (ICT) security controls in their ICT management regime.	
Physical Lifecycle *(Physical security)*	An organisation must establish, implement and maintain physical security controls in their physical management regine	

KPI Monitoring – integrate !

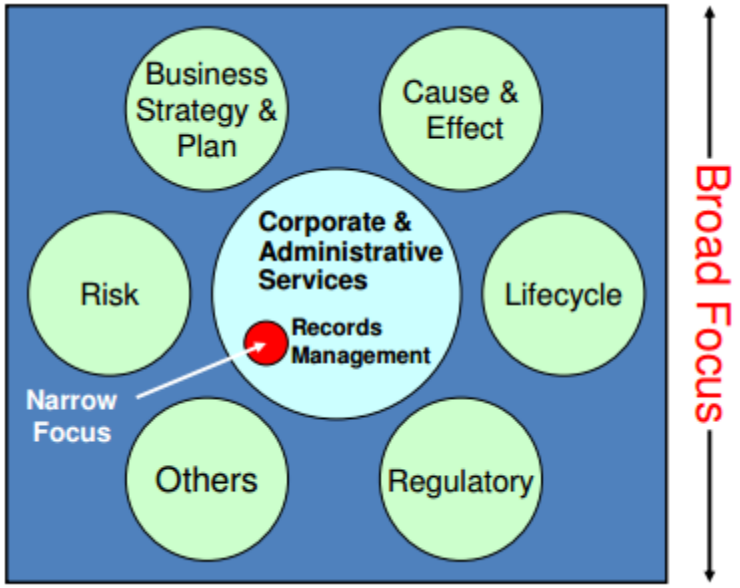
- KPIs assist the agency to define and measure progress toward agency goals and objectives. Once the agency has analysed its mission and defined its goals, it needs to measure progress towards those goals. KPIs provide a measurement tool.

KPI Characteristics

A KPI should be:

1) ***Relevant*** - consistent with the organisation's vision, strategy and objectives.
2) ***Focussed –*** a strategic value rather than non-critical.
3) ***Representative –*** appropriate to the organisation and its performance.
4) ***Realistic –*** fits into constraints and cost effective.
5) ***Specific –*** clear and focused to avoid misinterpretation or ambiguity.
6) ***Attainable –*** targets are observable, achievable, reasonable and credible under expected conditions as well as independently validated.
7) ***Measurable –*** can be quantified/measured and may be either quantitative or qualitative.
8) ***Used to identify trends –*** changes are infrequent and can be compared to other data over a reasonably long time.
9) ***Timely –*** achievable within the given timeframe.
10) ***Understood –*** participants know how their behaviours and activities contribute to overall goals.
11) ***Agreed –*** all contributors agree and share responsibility.
12) ***Reported –*** regular reports are made available to all stakeholders and contributors.
13) ***Governed –*** accountability and responsibility is defined and understood.
14) ***Resourced –*** the program is cost effective and adequately resourced throughout its lifetime.
15) ***Assessed –*** regular assessment to ensure that they remain relevant.

KPIs – Broad Approach



http://prov.vic.gov.au/wp-content/uploads/2012/04/1010G3-20130717.pdf

eassure INFORMATION INNOVATION

Brainstorm 4 - Develop KPIS for records security (10 mins)

eassure INFORMATION INNOVATION

KPI – setting them out

Goal 1 - Improve security of information

The first goal is to improve information governance and information security within [Name]. This is a multifaceted goal that encompasses such areas as policy, procedures, compliance, risk, delivery, systems, training and communications.

Issue	Actions	Timeframe	Owner	KPI	Priority
1. The [Name] Information Security Policy does not exist.	1. Develop Information Security Policy. As a minimum, reporting should include system statistics, help desk statistics, service delivery performance, compliance and resources.	Amend Policy by December 20XX.	Director Information Services.	Policy is amended by December 20XX. A bi-annual report to SMT.	2

Brainstorm 5: What do you do if you identify breaches?

Compliance Monitoring

2.4 Compliance Audits

Principle: Recordkeeping frameworks, procedures and practices must be audited at regularly to ensure the agency is operating in compliance with its recordkeeping procedures.

Requirement	Examples of Evidence
16. Recordkeeping procedures to be assessed by internal or external audits have been identified.	Risk assessment report that identifies recordkeeping activities and sections, divisions or business units where there may be a potential compliance risk. Documented review of procedures based on feedback from training and awareness programs. Audit program.
17. A recordkeeping audit program has been developed and endorsed by the senior executive with recordkeeping responsibility.	Documented approval and correspondence from appropriate delegates. For example the senior records manager, steering committee, governance group, director, executive director or the head of agency. Endorsed version of the audit program.
18. Recordkeeping audit procedures and criteria have been developed, and assessed following each audit.	Documented procedures outlining auditing steps and activities. Audit checklists. Audit program. Documented consultation and negotiation with divisional executives and key stakeholders to establish the audit schedule for specific areas, divisions, sections or business

Compliance Monitoring

		units. Intranet and email advice about workshops held to explain audit procedures, what is happening and when, and audit schedule advice for participants. Audit report. File notes on changes to audit schedule.
19.	**Results of recordkeeping audits and any audit recommendations have been documented, presented and reported to senior executives and relevant stakeholders.**	Audit report presented to senior executive and relevant stakeholders. Presentation of results. Correspondence to stakeholders. Audit action plan and item register. Correspondence to managers requesting actions on items listed as their responsibility, as documented in the audit action plan. Status reports.
20.	**The progress of recordkeeping audit recommendations are monitored and reported to senior executives.**	Correspondence to stakeholders. Audit action plan and item register from recommendations. Correspondence to managers requesting actions on items on audit action plan. Status reports. Schedule of workshops, seminars, refresher training to resolve action items. Final version of audit report.

Building Our Capability

- What can I do ?

Questions?