Review of the Victoria Police Security Incident Management Framework and Practices

Report of findings and recommendations

Issued January 2017

Commissioner for Privacy and Data Protection

VICTORIA State Government

This page is intentionally left blank.

Review of the Victoria Police Security Incident Management Framework and Practices

Report of findings and recommendations

Issued January 2017

Published by the Commissioner for Privacy and Data Protection
PO Box 24014
Melbourne Victoria 3001

January 2017

Also published on:
http://www.cpdp.vic.gov.au

DOCUMENT DETAILS	
Security Classification	UNCLASSIFIED
Dissemination Limiting Marker	Nil
Dissemination Instructions	For public release
Issue Date	January 2017
Document Status	Final
Authority	Office of the Commissioner for Privacy and Data Protection
Author	Projects and Operations

This page is intentionally left blank.

Contents

This page is intentionally left blank.

1 Introduction

The Office of the Commissioner for Privacy and Data Protection (CPDP) engaged KPMG to conduct a review of the Victoria Police Security Incident Management Framework for the protection of law enforcement data, including a critical assessment of organisational security incident management practices.[1]

Security Incident Management is a process 'aimed at minimising the immediate and long-term business impact of incidents'[2]. Victoria Police faces a broad range of security threats and vulnerabilities requiring constant identification, assessment and management – and a response proportionate to the risk.

An *adequate* response will take into account the nature, scope and severity of an incident, and will be, importantly, dependent on an organisation's risk appetite. The ability to implement pre-planned, comprehensive, well-rehearsed, and repeatable security incident management practices proportionate to this risk appetite is key.

With this in mind, the review identified a 'consistent set of factors to be considered by [Victoria Police] when determining its approach to the management of security incidents'[3] – a framework for best practice security incident management.

1 Reviews of Victoria Police Security Incident Management have previously been conducted by CPDP in November 2008 and December 2010.

2 *Security Incident Management: Good Practice Guide* (2015). Centre for the Protection of National Infrastructure, National Technical Authority for Information Assurance. p.1. Document accessed from https://www.ncsc.gov.uk/content/files/guidance_files/Security%20Incident%20Management%20(Good%20Practice%20Guide%2024)_1.2_0.pdf. Site accessed 2 December 2016.

3 *Security Incident Management* (2015). p.4.

2 Review purpose and methodology

2.1 Review purpose

The review aimed to determine the extent to which Victoria Police has implemented an effective Security Incident Management Framework.

A Security Incident Management Framework (SIMF) (Appendix A) has been developed by CPDP as both an operational and strategic platform to support and underpin the objectives of an effective incident management framework in *general*, with the document having the capability to be tailored as required to individual needs of an organisation. The SIMF is expected to be a primary control reference within the *Victorian Protective Data Security Standards* (VPDSS).[4]

KPMG was also tasked with validating the SIMF against benchmark national and international standards. CPDP considered that a validated SIMF would provide a sound basis for assessing current Victoria Police security incident management and practices.

The SIMF models controls, and control objectives, across the four phases of the security incident lifecycle being:

- Preparation – effective incident response capability through planning and preparation
- Detection – capability to assess events and identify incidents
- Handling – capability to respond to identified incidents in a timely manner
- Prevention – capability to reduce the business impact of a security incident and to prevent incidents from re-occurring.

Victoria Police have obligations regarding effective security incident management under the *Standards for Law Enforcement Data Security* (SLEDS), specifically Standards 32 and 33, Security Incident Management. Effective security incident management objectives are explicitly stated, being:

- *Standard 32 objective - To allow timely and corrective action to be taken in the event of an information security incident in order to protect law enforcement data and reduce the impact and likelihood of damage caused by the failure of information security controls,* and;
- *Standard 33 objective - To ensure feedback on incidents and that information security incident management procedures can be continually improved so that future incidents are better managed.*[5]

The SLEDS are authorised under the *Privacy and Data Protection Act* 2014 and are binding on Victoria Police.

4 *Victorian Protective Data Security Standards*. Standard Seven – Security Incident Management. Accessed from www.cpdp.vic.gov.au.

5 *Standards for Law Enforcement Data Security* (SLEDS) 2014. Security Incident Management, Standards 32 and 33. Accessed from www.cpdp.vic.gov.au.

2.2 Review methodology

The review undertook an assessment of the following components impacting on, or influencing, security incident management and practices within Victoria Police. These components included:

- all relevant Victoria Police security incident management policies and guidelines
- overarching governing legislation and standards (eg. SLEDS and the Australian Government Protective Security Policy Framework)
- current Victoria Police governance arrangements and statements of strategic direction
- Victoria Police security incident subject matter expertise
- current Victoria Police security incident lifecycle across preparation, detection, handling and prevention within all security domains (physical, personnel, information and ICT).

The review included:

- stakeholder consultations within Victoria Police
- consultations with and document review of other jurisdictions (United Kingdom, New Zealand and South Australia).
- a sample assessment of Victoria Police security incidents
- attendance at a Victoria Police i-SAG[6] meeting
- a high-level review of the SIMF against national and international benchmark standards
- a capability maturity assessment (Appendix B) of Victoria Police's information security management and practices against the security incident lifecycle phases.

6 Information Security Assessment Group.

3 Findings

Overall, KPMG provided a maturity assessment of Victoria Police information security incident management and practices as 'Repeatable', meaning that the process is documented sufficiently such that repeating the same steps may be attempted.[7]

The assessment by KPMG also delivered a series of detailed observations and findings. CPDP and Victoria Police evaluated KPMG's assessment, and identified and agreed upon five high-level findings fundamental to improving security incident management and practices within Victoria Police.

These findings form the basis of the recommendations made in this report.

For the sake of completeness, the report also recommends that Victoria Police adopt and implement the SIMF in order that Victoria Police's security incident management and practices be aligned with those of the wider Victorian public sector as implementation of the VPDSS takes place.

To further support this recommendation, the review has linked each finding to the relevant Standard for Law Enforcement Data Security, and also mapped against the corresponding Standard/s within the Victorian Protective Data Security Framework (VPDSF).[8] The mapping highlights the relevance of the findings against what is *currently* expected under the SLEDS, and their *ongoing applicability* to information security incident management under the VPDSF.

3.1 Fragmented documentation exists for security incident management and practices

SLEDS – Std 1
VPDSF – Std 3, 7

Good security incident management documentation underpins an organisation's ability to safeguard its assets through supporting and maintaining the development of:

- strong governance arrangements
- effective risk management processes
- a positive security culture amongst staff
- business objectives including business continuity
- opportunities for continuous improvement.

Without comprehensive and effective documentation, these capabilities can become eroded and ineffectual.

Documentation should be concise and aim to provide clear direction. It should also provide a basis for training in security awareness and for reinforcing and measuring compliance with policy and legislation. Furthermore, new or altered policies and procedures need to be communicated to all employees to ensure they are properly implemented.

The review identified fragmented information security documentation across organisational and station-level policy and process, with no single document providing a comprehensive overview of the Victoria Police information security incident management process. The review also highlighted complex, lengthy, and often duplicated, documentation, with different documents seeking to establish different security incident management roles and responsibilities. The result is that the primary source

7 It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained in times of stress.

8 This mapping is one way (SLEDS to VPDSF) as the SLEDS are the current regulatory requirement for Victoria Police pending their transition to the VPDSF in 2017.

of advice and guidance is often obfuscated. This finding is supported by site inspections of Victoria Police facilities undertaken by CPDP where employees frequently reported that it is difficult to 'see the wood from the trees' with regards to policy and process documentation.

The review reinforced that fragmentation of documents presents a significant risk to effective communication of, and compliance with, information security management processes and obligations. For example, discussion of reporting processes and associated roles (see Finding 3.2) is duplicated across several organisational policy documents. In addition, many documents reviewed have not been updated for several years, with a number dating back to 2011.

Multiple contesting documents also create the potential for issues with consistency when roles and responsibilities are changed (refer to Finding 3.4).

CPDP notes the advice from Victoria Police that organisational policy (the *Victoria Police Manual* or VPM) is currently undergoing significant review, including restructure, driven by employee confusion around the application of, and adherence to, *Policy* (VPM-P) and *Guidance* (VPM-G) material. It is also relevant to highlight that the Information Management, Standards and Security Division (IMSSD), the primary specialist information security capability within Victoria Police, does not drive the layout of the VPM. As such, the review observed that IMSSD change-management around information security policy and operating procedure functions in a difficult environment driven by organisational bureaucracy (including difficulty in influencing decision-making), and resource constraints (time, personnel and financial).

Through the review process, Victoria Police advised that organisational policy is both slow to change and to implement. Whilst recognising these difficulties, Victoria Police need to develop a more agile and responsive approach to security incident management. However, IMSSD have the potential to drive change at the frontline through the provision of primary, authoritative, and easily accessible guidance documentation.

Recommendation One

That Victoria Police review, validate, and update security incident management policies ensuring they are simplified, integrated and communicated to all stakeholders.

3.2 Security incident awareness and reporting is inconsistent and ineffective

SLEDS – Std 7
VPDSF – Std 6, 7

Promoting a strong security awareness and learning culture is essential to supporting and encouraging the reporting of security incidents. This, in turn, facilitates the capture of sufficient and robust data and the identification of root causes of problems. Aligning closely with other key findings of this report, *effective* security incident *awareness* is linked to the need for good documentation, clear and defined roles and responsibilities, and effective risk management – as well as the crucial role of training and education. The central outcome from improved awareness and reporting is the ability to feed 'lessons learnt' back into the *prevention* phase / focus of the security incident lifecycle, and promote continuous improvement.

The review highlights low organisational awareness around information security incident detection and reporting, whilst noting positive signs of progress. Pivotal to opportunities for improvement is a communication strategy focussed on simple messaging and engagement across:

- information security risks (refer to Finding 3.3)
- security incident management reporting obligations, and
- the security incident notification process.

The review found that IMSSD require access to a specialist communications and organisational change capability to support the Division's wider educative function. Analysis of the CPDP longitudinal survey[9] data against the Victoria Police Cultural Change project highlighted an inability to correlate positive change markers within the data to tangible programs and projects.

This finding is consistent with CPDP site inspections and the data from the CPDP longitudinal survey. Victoria Police employees indicate confusion around what constitutes an information security incident (such as the potential for incidents to occur, as distinct from, actual incidents having occurred), with the threshold for reporting being unclear due to the self-assessment of intent (intentional or unintentional, indications of malfeasance of criminality etc.). If there is any confusion around reporting, employees are less likely to appreciate risk; and with no appreciation of risk, it is likely that less reporting will be initiated (see Finding 3.3).

Force-wide information security training programs and awareness campaigns are undertaken by IMSSD, however are dependant on resource capacity and also any incident catalyst (ie. a primary focus resulting from a serious incident, or an identified thematic pattern or incident trend). CPDP notes that the Victoria Police Security Incident Registry (SIR) undertakes reactive / remediation training after an incident has occurred. These activities are an integral part of a *Plan, Do, Check, Act* continuous improvement lifecycle model.

However, security incident training programs only form part of a wider and diverse organisational training schedule attempting to manage competing demands, expectations and deliverables. With Information Management and Information Security (IM&IS) now forming part of the Victoria Police 'CompStat' process, requirements for Stations, Police Service Areas (PSAs) and Regions to report against and meet IM&IS expectations appear to be increasing faster than organisational awareness and acceptance of best-practice information security.

However improvements to organisational awareness are being attempted. IMSSD are currently undertaking an ongoing project around cultural change that includes program initiatives such as the roll-out of the IM&IS portfolio holders, and dedicated, mandatory online information security training. The review highlights that the active promotion of a culture of incident reporting is contributing positively to overall levels of information security awareness, including a growing trend of incident

9 CPDP longitudinal survey of Victoria Police information security culture and practices 2012-2016

reporting by members. However, there is scope for Victoria Police to continue to strengthen awareness across the organisation, as consultation participants commonly considered that it was the lack of awareness, rather than a cultural reluctance to report, that constituted the primary barrier to more effective incident identification and reporting.

The review emphasises the importance of a strong, centralised approach to information security awareness training to ensure consistency in content and delivery. While IMSSD have developed, and continue to develop, a number of tools to support information security incident management, there is a requirement to maintain the focus on training including the development of a comprehensive, varied, and innovative suite of initiatives.

Recommendation Two

That Victoria Police undertake force-wide Security Incident Management training focusing on:

- what constitutes a security incident
- what are members' reporting obligations
- the reporting process.

3.3 Limited visibility, and definition, of the link between security incidents and risks

SLEDS – Std 31, 33
VPDSF – Std 2, 7

Risk management is 'a logical and systematic process of identifying, prioritising, treating, communicating and monitoring events that may prohibit an organisation from achieving its objectives [...]'.[10] A comprehensive and effective risk management process is important to enable and enhance the identification and appropriate treatment of risks through:

- the development, documentation, implementation and regular review of risk management policy and process
- ensuring the successful application of the risk management policy through communication in a form and manner that is relevant, accessible and understandable
- the maintenance of 'line of sight' between risk managers and risk (at both the frontline and organisational level).

The review underscores a need for Victoria Police to strengthen the link between security incidents and risk. Limited security incident awareness (see Finding 3.2) and the corresponding failure to report security incidents severely limits Victoria Police's ability to conduct an adequate risk assessment. Therefore Victoria Police's risk posture remains undefined. This has direct consequences for training and resourcing in security incident management.

Consultations identified a separation and isolation of organisational risk assessment, governance, management, and capacity across various roles and functions responsible for managing security incidents.

To highlight the importance of integrated security incident risk management, the Chief Risk Officer (CRO), as an Executive position, has oversight of three enterprise risks relating to information security. Visibility of information security management across Victoria Police is essential to the function of the CRO. The CRO sits on the Security Committee (focusing on information, physical and personnel security). Additionally, the CRO reports to Executive Command and has recently established regular meetings with the Agency Security Executive (ASE) in order to build a shared understanding of security risks and the work being undertaken to mitigate them.

The Chief Information Officer (who also holds the position ASE) maintains oversight of all security incidents within Victoria Police. The engagement of the role and function of the ASE at Executive Command level helps both maintain Organisational awareness and drive Executive endorsement of security incident management, and any relevant Organisational cultural change initiatives (See Finding 3.2).

IMSSD, as the central point for security incident management in Victoria Police, has developed the capability to liaise with other risk and planning units within Victoria Police about the progress of information security related risks, and the implications of incidents across all four security domains, from a holistic enterprise risk perspective. (Also refer to Finding 3.4)

Frontline members indicated to the review that current processes for making resourcing decisions about identified enterprise information security risks appears to be not as effective as it could be. Again, this observation is supported by findings from the CPDP site inspections and the longitudinal survey - that organisational issues often play out at, and impact on, the local level – with the review underscoring the requirement, organisationally, for more sophisticated incident analysis to predict and guard against future risk.

10 *Standards for Law Enforcement Data Security* (2014). Chapter Eleven – Risk Management. p.67.

Recommendation Three

That Victoria Police align and integrate security incident management and practice with the organisational risk management framework.

3.4 Security incident roles and responsibilities are not well defined or understood

SLEDS – Std 3
VPDSF – Std 3, 5, 7

The security incident management environment can be a complex, and often changing, landscape. Sound governance involves, in part, clear direction and the assignment and acknowledgement of responsibilities in security incident management and practice. Clearly detailing SIM roles and responsibilities is important as it:

- provides clear direction and visible support for security incident management initiatives, including identifying SIM goals (tailored to organisational requirements)
- ensures SIM policy is developed, approved and reviewed
- ensures the availability of required SIM resources
- assigns specific roles and responsibilities for SIM and practices
- initiates plans and programs to maintain SIM and practices
- ensures that the implementation of SIM controls is coordinated.

Review observations highlight three distinct tiers of stakeholders engaged within the Victoria Police security incident management landscape. These tiers are:

1. Internal Victoria Police stakeholders
2. External stakeholders responsible for regulating protective data security and having a primary focus on (Victorian) law enforcement agencies – CPDP
3. Other oversight, regulatory, and specialist bodies.[11]

The review underlines that security incident management functions, activities, objectives and expectations of respective organisations are not well defined. Furthermore, there was confusion around the implementation and management of stakeholder relationships, including lines of communication, communication content, and the level of collaboration and cooperation required between internal and external stakeholders.

This lack of clear, defined SIM roles and responsibilities is also impacting negatively on the development and maintenance of future or existing protocols (such as the *Escalated Reporting Protocol*[12] currently in place between IMSSD and CPDP).

Victoria Police are actively working to strengthen both engagement and understanding across the organisation, recognising that this is pivotal to supporting the implementation of a holistic enterprise-wide approach to information security incident management – with the primary activities being SIM role identification, definition and promotion.

It is a certainty that ongoing and dedicated organisational support towards SIM capacity building is fundamental to enabling Victoria Police SIM capabilities. Building, and maintaining, capability around security incident management functions, activities, objectives and expectations is imperative to not only address organisational accountabilities, but also those of oversight and regulatory bodies like CPDP.

Recommendation Four

That Victoria Police identify, define and document all security incident management roles and responsibilities (such as within a RACI model).

11 For example IBAC, VAGO, PROV, VMIA etc

12 The Protocol aids the reporting of information security incidents by Victoria Police to CPDP

3.5 Victoria Police does not have an effective or authorised SIMF in place

SLEDS – Std 32
VPDSF – Std 7

An effective and robust SIMF details and ensures a consistent approach to the management of security incidents by supporting the *Plan, Do, Check, Act* model of continuous improvement lifecycle. Importantly, a SIMF enables the systematic identification of opportunities to mature protective data security practices by providing organisational focus on, and impetus for, increasing security incident management capacity, capability and flexibility.

The review finds that Victoria Police's security incident management is not optimised towards best practice, including by not currently having an adequate, robust SIMF. The key findings in this report indicate ongoing and elevated risks around current security incident management and practice including:

- the loss of confidentiality, integrity and availability of systems of data
- a loss of reputation / credibility with stakeholders
- disorganisation and inefficiency driven by protracted and/or poorly coordinated incident management activity
- security incident management communication that is not relevant, accurate or timely
- incidents reoccurring through not understanding risk, or applying lessons learnt.

As part of the wider review expectations, KPMG validated the attached SIMF against national and international benchmark standards and therefore it is ready for broader implementation. The validated SIMF forms a consistent, and best practice, model that Victoria Police should adopt and deploy.

Recommendation Five

That Victoria Police agree to adopt the SIMF and develop a roadmap for its implementation, including milestones and timelines.

4 Recommendations

Recommendation One

That Victoria Police review, validate and update security incident management policies ensuring they are simplified, integrated and communicated to all stakeholders.

Recommendation Two

That Victoria Police undertake force-wide security incident management training focussing on:

- what constitutes a security incident
- what are members' reporting obligations
- the reporting process.

Recommendation Three

That Victoria Police align and integrate security incident management and practice with the organisational risk management framework.

Recommendation Four

That Victoria Police identify, define and document all security incident management roles and responsibilities (such as within a RACI model).

Recommendation Five

That Victoria Police agree to adopt the SIMF and develop a roadmap for its implementation, including milestones and timelines.

5 Management Action Plan

CPDP REC NUMBER	REPORT REC NUMBER	ACCOUNTABLE	RESPONSIBLE	DATE	COMMENT
262	1	Director, Information Management and Assurance	• Director, Information Management and Assurance	30 June 2017	Agreed – Draft to PLO process by date
263	2	Director, Information Management and Assurance	• Inspector, Security Incident Registry	30 December 2017	Agreed
264	3	Director, Information Management and Assurance	• Inspector, Security Incident Registry • Chief Risk Officer	30 December 2017	Agreed
265	4	Director, Information Management and Assurance	• Project Director, ICT Operating Model Review	30 December 2017	Agreed
266	5	Director, Information Management and Assurance	• Inspector, Security Incident Registry	30 June 2017	Agreed

Unclassified

6 Appendices

Appendix A – Security Incident Management Framework

PHASE			CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
A)	Preparation	Organising an effective security incident management capability requires planning and preparation	A.1	Definitions	Having clear definitions in the organisational context for a security event and incident	A1.1	Events & Incidents	Security events and incidents have been well defined and the differences clearly articulated	A document defining what constitutes a security event and an incident
						A1.2	Thresholds	Thresholds have been defined for when a security event becomes an incident	A document providing the criteria when a security event becomes an incident
						A.1.3	Categorisation	Criteria to categorise security incidents have been defined	A document defining the criteria and categories for security incidents
			A.2	Requirements	Organisational context and requirements must be understood and defined	A2.1	Obligations register	Regulatory, legal and administrative obligations have been registered	A register showing all obligations

Unclassified

PHASE	CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
				A2.2	References	Contractual requirements and other agreements have been referenced	A register showing contractual or other requirements
	A.3	Policy	To state the organisational intent, objective and to provide direction for the effective implementation of a Security Incident Management Framework	A.3.1	Policy - Statement of management commitment	Senior management have demonstrated their commitment and support to ensuring the effectiveness of the Security Incident Management Framework	Executive sponsorship and buy-in for the establishment of a Security Incident Management Framework Embedding policy across the organisation Management endorsement on Policy. (Look for meeting minutes where policy endorsement was tabled. Staff communications from senior management in relation to policy, etc.)

Unclassified

PHASE	CONTROL	CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
			A.3.2	Policy Direction & Objective	The purpose and the objectives of the policy have been clearly articulated	Purpose and objectives are articulated in a policy document
			A.3.3	Ownership	Ownership for policy has been assigned	Statement of ownership in the policy
			A.3.4	Policy Review	The policy has been reviewed in line with the organisations policy governance framework. In absence of such a framework, the review is done at least annually	A document trail for policy review (can be email, agenda item(s) or any other evidence of review activity)
			A.3.5	Communication	The policy has been communicated to all relevant internal and external parties	Specific communiqués to internal and external parties about policy
			A.3.6	Interdependencies	Relationships and dependencies to other policies and procedures have been documented	A document showing the relationships across the organisation

Unclassified

PHASE	CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
	A.4	Plan	To provide the resources and a roadmap for the implementation of the Security Incident Management Framework	A.4.1	Roadmap	A roadmap for maturing security incident management capability	A document showing the planned activities over time to mature security incident management capabilities. Requires the organisation to understand the need and areas for capability improvements
				A.4.2	Performance measures	The effectiveness of the Security Incident Management Framework has been monitored through defined performance measures	Defined performance measures and evidence of actual data collection and response to collected data
				A.4.3	Executive approval	Executive have approved the elements of the plan	Meeting minutes or any other evidence showing direct (not implicit) approval of improvement plan

PHASE	CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
	A.5	Internal Standards	To support the policy objectives	A.5.1	Internal standard set	A set of supporting internal standards have been documented in support of the policy objectives specifiying baseline expectations of what must be done	Documented internal standards detailing what must be done to achieve the policy objectives
				A.5.2	Coverage	Internal standards cover the Security Incident Management Lifecycle	Elements of internal standards are defined across the lifecycle (i.e. Preparation, Detection, Handling and Prevention)
				A.5.3	Prioritisation	Internal standards that define how to prioritise specific security incident categories	An internal standard that articulates how incidents are prioritised

Unclassified

PHASE	CONTROL	CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
			A.5.4	Communication	Internal standards that define how and when to communicate with internal and external parties – e.g. oversight bodies, regulators, Media, Service Providers, Other Agencies	A specific internal standard that details communication protocols
			A.5.5	Risk alignment	The internal standards link to the organisational risk management framework	Evidence that the security incident management framework has been integrated with the organisational risk management framework (including internal standards)
			A.5.6	Ownership	Ownership for internal standards has been assigned	Statement of ownership in the internal standard

PHASE	CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
				A.5.7	Review	The internal standards are reviewed on a regular basis or if significant events have occurred (e.g. incidents or changes to the organisation)	Evidence of review activities, e.g. email trails, revision history
	A.6	Processes	To provide detailed and pre-defined guidance on internal standards	A.6.1	Coverage	Processes supporting the activities of all security incident management lifecycle phases	Processes supporting standards across all security incident management lifecycle phases (Preparation, Detection, Handling, Prevention) Processes address coverage across the organisation
				A.6.2	Prioritisation	Processes have been defined to support the prioritisation of specific security incident categories	Detailed instructions exist around the prioritisation of incidents

Unclassified

PHASE	CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
				A.6.3	Communication	Processes that outline the communication protocol in accordance with the internal security standards	Detailed communications protocols, showing who can say what and when
				A.6.4	Ownership	Ownership of each process has been assigned	Statement of ownership in internal documentation
				A.6.5	Review	The processes are reviewed on a regular basis along with the internal standards they support	Evidence of review activities, e.g. email trails, revision history
	A.7	Resources	To provide the required tools throughout the Security Incident Management Lifecycle	A.7.1	Templates	Templates have been defined such as e.g. Incident Fact Sheet, Post Incident Reports	Prepared templates such as Fact Sheets, Post Incident Reports, etc.

PHASE	CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
				A.7.2	Toolkits	Required tools to manage the Incident have been identified, e.g. facilities, systems, people	Evidence of tools to support the security incident management processes
				A.7.3	Contact Lists	Contact lists have been pre-compiled for all relevant internal and external stakeholders	Contact lists showing details of every key stakeholder and secondary contacts allowing 24/7 access to individuals and services
	A.8	Roles & Responsibilities	To ensure that all internal and external parties understand roles and responsibilities	A.8.1	Team Model	The security incident management team model has been defined (e.g., Centralised, Distributed) addressing both oversight / management and response	Documented details of the security incident management team model(s), including security incident management response

Unclassified

PHASE	CONTROL	CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
			A.8.2	Roles & Functions	Each participant has a defined role and function	Every role / function is supported by a defined and documented RACI model
			A.8.3	Authority	The authorities for decision making have been defined	A document that states the authority for decision making for any financial, reputational, operational, legal & regulatory implications
			A.8.4	External Parties	The roles and responsibilities of external parties have been defined	A document showing the roles and responsibilities of external parties
			A.8.5	Consumers	The needs of consumers in the context of incident management have been defined and are understood	A document showing the need (information / data) for consumers (customers) during a security incident – e.g. both suppliers and recipients

PHASE	CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
				A.8.6	Dependencies	Dependencies on services and resources (both within and beyond the organisation) have been defined - e.g. Legal, IT Support, Regulatory, Facilities, etc.	A document showing the dependencies on and by other parties/services
	A.9	Skills, training and awareness	Ensure that all relevant parties are aware, well prepared and skilled in Security Incident Management	A.9.1	Skills and competencies	Stakeholders have been selected with suitable skills, matching their roles and responsibilities in the Security Incident Management Framework and bring a cross-section of business knowledge to the team	Composition of the security incident management team reflects key workgroups across the organisation (e.g. corporate communications, HR, Financial, Facilities, Executives, Records Management, ICT) Staff have completed relevant security incident training

Unclassified

PHASE			CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
						A.9.2	Training	A training plan has been documented addressing the ongoing training needs of the security incident management team(s)	A training plan detailing the actions, activities and focus areas of those involved in security incident management
						A.9.3	Awareness	A security incident awareness program has been defined and implemented ensuring all internal and external stakeholders are aware of the Security Incident Management Framework	Evidence of communications to internal and external stakeholders Spot-check of actual awareness of the security incident management framework
B)	Detection	The capability to assess events and identify security incidents	B.1	Threat Intelligence	Proactively detect any threats and vulnerabilities	B.1.1	Threat Analysis	External/Internal threat analysis is performed to establish an understanding of the threat environment and in turn detect changes	Evidence of Threat Analysis, e.g. Threat Reports, Threat & Risk Workshops

PHASE	CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
				B.1.2	Frequency	Threat Analysis has been frequently performed. The schedule must be defined by the business based on the organisational context. Criteria has been defined for unscheduled analysis activities	Document detailing the frequency of Threat Analysis including criteria for unscheduled reviews based on changes to the threat environment
				B.1.3	Quality/Reliability	Threat assessments have determined the reliability and quality of the information being analysed. This information has been provided with the threat report	Quality/Reliability statement of the threat intelligence is articulated in any threat reporting
	B.2	Vulnerability Analysis / Attack Vectors	Vulnerabilities and attack vectors are understood in the context of existing and potential threats	B.2.1	Vulnerability Scans	Perform regular analysis for vulnerabilities and attack vectors, based on the existing and potential threats	Vulnerability assessment reports

Unclassified

PHASE	CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
	B.3	Security Monitoring	Timely detection of events and security incidents	B.3.1	Indicators	Security incident indicators and precursors have been defined	A document stating the precursors and security incident indicators
				B.3.2	Event Monitoring	Events are assessed / monitored for defined indicators and precursors	Evidence that events are assessed / monitored using the defined indicators/ precursors
				B.3.3	Testing	Any new defined security incident indicators or precursors have been tested against the existing security events	Evidence that retrospective review of security events was performed when security incident indicators or precursors have changed

PHASE			CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
						B.3.4	Alerting	Alert thresholds for security incidents are documented (both automated and via user reporting)	Examples may include: • A system which includes an automated tool with a built in alert function • Significant changes to a 'factor area' for a security clearance holders
C)	Handling	The capability to respond to security incidents in a timely manner	C.1	Triage	Assess the security incident elements to determine how to best manage it	C.1.1	Team Model	Utilising the pre-defined team model, to triage the security incident	Evidence in form of corporate communications (e.g. internal and external emails, Intranet communications, etc.)
						C.1.2	Process	Consider the elements / characteristics of the security incident and follow pre-defined response and management processes	Follow process documents that outline what to do in the case of particular security incidents

Unclassified

PHASE	CONTROL	CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
			C.1.3	Timeliness	Assess security incidents in a timely manner (ensuring 24/7 response where required)	Process review showing that reported security incidents are addressed within a reasonable timeframe
			C.1.4	Parameters / Scope	Establish a terms of reference for particular security incidents including response parameters (where required)	E.g. 'Terms of reference' document for a particular security incident
			C.1.5	Register	All reported security incidents are recorded with an assessment outcome	A register showing recorded and accompanying assessment outcomes
			C.1.6	Prioritisation	All security incidents have been prioritised according to relevant internal standards	A record of the priority assessment is captured in the Security Incident Register

Unclassified

PHASE	CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
				C.1.7	Categorisation	All recorded security incidents are categorised	A record of the category is captured in the Security Incident Register
				C.1.8	Asset owners	Asset owners are identified during the triage assessment (if applicable)	A record of the asset owner is captured in the Security Incident Register
	C.2	Analysis	To ensure security incidents are analysed as information becomes available	C.2.1	SME Engagement	Engage suitable subject matter experts (SMEs) from relevant areas and bring these SMEs into the security incident response process	A process document showing how SMEs are engaged
				C.2.2	Business Impacts	Business impacts resulting from the security incident are assessed	A process document showing that business impacts are assessed Fact sheets from past events showing business impact assessments

Unclassified

PHASE	CONTROL	CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
			C.2.3	Ongoing analysis	As additional information becomes available, the original assessment is re-considered to identify whether the security incident needs to be prioritised or response activities adjusted	Documentation from past incidents showing risk considerations of new information – e.g. risk assessments throughout the incident lifecycle Requests for information to support analysis
			C.2.4	Process	Follow pre-defined communication protocol according to the security incident elements / characteristics	Information flows have been controlled and pre-defined (i.e. who can talk to whom and when) during the handling phase

Unclassified

PHASE	CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
	C.3	Containment	Prevent further damages from the security incident in a controlled fashion	C.3.1	Containment Strategies	Follow pre-defined containment strategies set out under internal standards / processes	Evidence that the document outlining the containment strategies has been followed (e.g. wipe & restore, monitor and observe, etc.) Evidence of consideration given to issues such as Forensics, Personnel Security, Disaster Recovery, Business Continuity Management
				C.3.2	Authority	Follow pre-defined decision authorities for the containment of the security incident	Evidence that the document outlining the decision authorities for the containment strategy has been followed
	C.4	Rectification	Address issues leading to the security incident	C.4.1	Controls	A process has been defined to rectify any issues or remediate controls that failed to prevent the security incident from occurring	A process document that shows how to fix/ rectify control failures for the security incident

Unclassified

PHASE	CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
				C.4.2	Scope	Rectification has considered areas that are not impacted but rely on the same controls	A process showing that after controls failures, similar controls or controls in other areas are reviewed Evidence from past events showing that such review are performed
	C.5	Recovery	Recover from the security incident and resume normal business operations	C.5.1	Business Continuity	Initiate Business Continuity Plan	Evidence of linkage to Business Continuity Management
				C.5.2	Recovery Strategies	Follow pre-defined restore strategies outlined in internal standards / processes	Evidence that the document outlining recovery strategies has been followed

Unclassified

PHASE	CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
	C.6	Communication / Engagement	To provide accurate, factual and timely information to stakeholders	C.6.1	Communication / Engagement Plan	Follow pre-defined engagement plan	Evidence that the documented engagement plan including: • listing all relevant stakeholders and their information requirements • communication channels (e.g. email, phone, Intranet, etc.) has been followed
				C.6.2	Frequency	Ensure frequent status updates are provided to key stakeholders	Evidence that key stakeholders have been updated on the status of security incidents
				C.6.3	Authority	Follow the pre-defined communications plan that identifies who has the authority to communicate to different stakeholders	A statement of authority covering all identified recipients of communication

Unclassified

PHASE			CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
D)	Prevention	The capability to reduce the business impact of a security incident and to prevent incidents from re-occurring	D.1	Post Incident Review	To provide direct feedback on the effectiveness of security incident management	D.1.1	Review	A process has been defined to perform a subjective and objective assessment of security incident management	Evidence that a review has occurred after a security incident
			D.2	Collecting Incident Data	To support the ongoing improvement of the security incident response capability	D.2.1	Incident Register	Details about the security incident have been recorded in a register	A security incident register containing performance metrics such as categorisation, business impact, time per incident, review outcomes and recommendations
			D.3	Awareness	To ensure that all relevant stakeholders are aware of any updates to the Security Incident Management Framework	D3.1	Communications	All stakeholders with an identified role in the SIMF have been made aware of any changes or updates to it	Evidence of communications about changes to staff when after the last revision of standards/processes

Unclassified

PHASE	CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
	D.4	Information Sharing	To ensure relevant stakeholders are provided relevant information about the security incident	D.4.1	Information Exchange	Follow the pre-defined process that identifies any stakeholders who may not have been directly involved during the handling phase	A document showing non-involved parties and their information needs - e.g. CPDP, DPC (ESB), DSD, AFP, AusCERT, other linked agencies This process relies upon pre-defined documented information sharing arrangements with such agencies
	D.5	Evidence Retention	To ensure evidence relating to the security incident is retained in a suitable manner (if required)	D.5.1	Retention & Preservation	Retention and preservation of evidence relating to the security incident has been defined in accordance to organisational internal standards / processes as well as any other legal and regulatory requirements	Clear articulation of retention/ preservation requirements of evidence obtained during the security incident

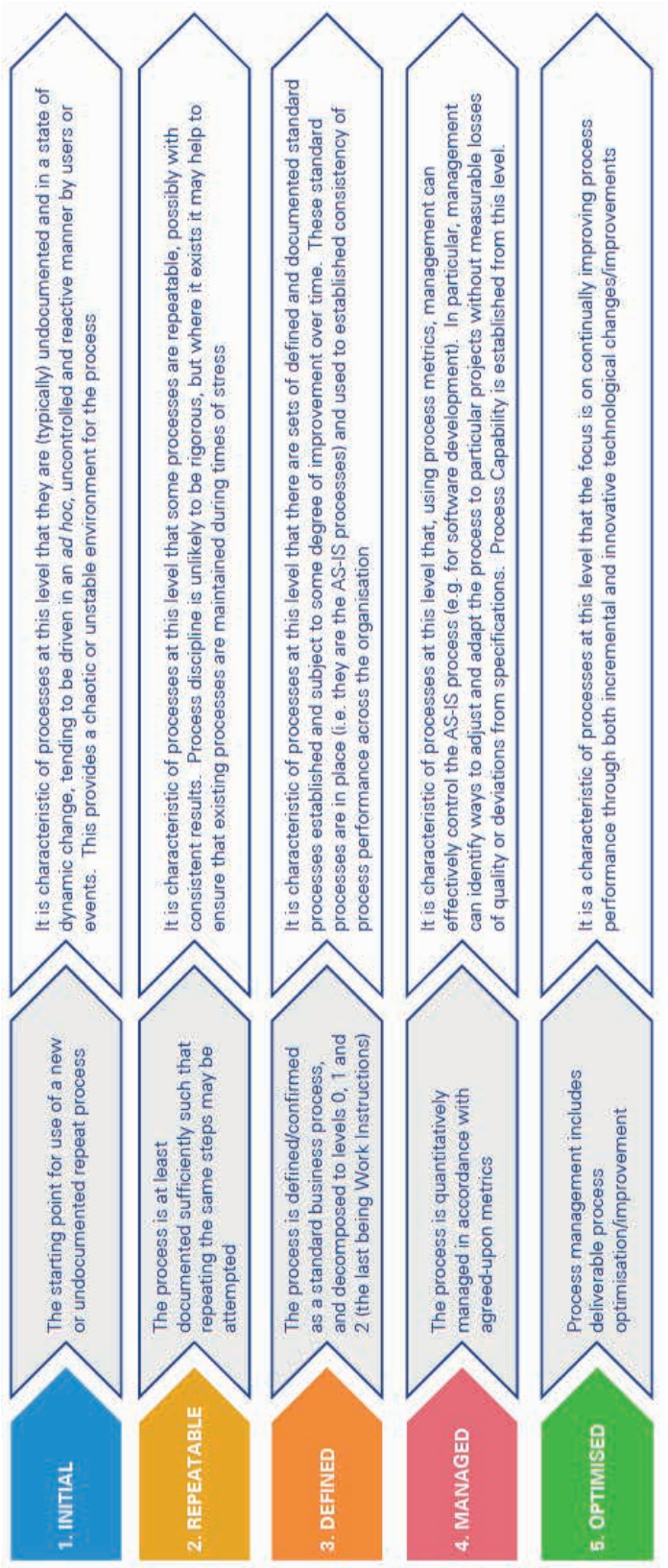
Unclassified

PHASE	CONTROL		CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
	D.6	Lessons Learnt	To ensure security incident response activities are reviewed for lessons learnt	D.6.1	Incident Review	A process has been documented to ensure that the security incident is reviewed for lessons learnt	Evidence of review activities since the last recorded security incident
	D.7	Audit & Reviews	To ensure the ongoing effectiveness of the SIMF	D.7.1	Scope	The scope for audits and reviews of the security incident management framework is clearly defined	A clear definition of scope
				D.7.2	Coverage	Audit and reviews cover all components of the Security Incident Management Framework	Evidence of audit activities across components of the Security Incident Management Framework
				D.7.3	Linkage to Threat/ Risks	Audit and reviews of the Security Incident Management Framework take into account existing risks and threats	Audit planning considers recent events, current identified threats and risks

PHASE	CONTROL	CONTROL OBJECTIVE		EXPECTED ELEMENT	DESCRIPTION	EXAMPLES/ ARTEFACTS
			D.7.4	Frequency	The frequency for audit and reviews of the security incident management framework have been defined (i.e. conducted on a regular basis or if significant events have occurred)	A document stating the frequency for audit/reviews, taking into account the need for unscheduled reviews to respond to significant events / incidents

Unclassified

Appendix B – Capability Maturity Model



Commissioner for Privacy and Data Protection

VICTORIA State Government