Office of the Victorian Information Commissioner

INFORMATION FOR
AGENCIES and BODIES

1300 00 6842 | ovic.vic.gov.au

Guide to developing an Information Security Incident Management Framework (ISIMF)

Version V2.0

This guide has been developed to assist organisations in addressing Standard 6 of the Victorian Protective Data Security Standards (**VPDSS**).

It’s important to note, that the Information Security Incident Management Framework (**ISIMF**) attributes represented in this guide provide a comprehensive approach to information security incident management, with the expectation that organisations build their own business processes around some of the controls presented below.

Given the wide variety and nature of organisations operating across the Victorian Public Sector (**VPS**), OVIC recognises that governance arrangements can take many forms. As such, organisations should contextualise the ISIMF attributes relative to their size, resources and risk posture.

Phase			Activity		Objective	Controls			Examples/Output
A	Plan and Prepare	Organising an effective information security incident management capability requires planning and preparation	A.1	Definitions	To clearly define the organisational context for an information security event and incident	A.1.1	Events and incidents	Define and articulate the differences between information security events and incidents	A definition with examples of what constitutes an event and an incident
						A.1.2	Thresholds	Define the thresholds for when an information security event becomes an incident	Criteria defining when an event becomes an incident
						A.1.3	Categorisation	Define the criteria to categorise information security incidents	Criteria defining the categories for information security incidents
			A.2	Requirements	To understand and define the organisational context and requirements	A.2.1	Obligations register	Register the organisation’s regulatory, legal and administrative obligations	List of all obligations
						A.2.2	Third party requirements	Register any contractual requirements and other agreements	List of approved arrangements with third parties to contact/ utilise to manage an incident (e.g. contracts with incident responders/ forensic services, assistance services from other agencies such as Vic Gov CIRS)

Phase			Activity		Objective	Controls			Examples/Output
			A.3	Policy	To state the organisational intent, objective and to provide direction for the effective implementation of an ISIMF	A.3.1	Policy statement of management commitment	Commitment to the Information Security Incident Management Framework by senior management	Executive sponsorship and buy-in for the establishment of an ISIMF Embedding policy across the organisation Management endorsement on policy (e.g. meeting minutes) Staff communications from senior management in relation to policy
						A.3.2	Policy direction and objective	Articulate the purpose and the objectives of the policy	An artefact stating the purpose and objectives
						A.3.3	Ownership	Assign the owner for policy	An artefact stating the owner of the policy
						A.3.4	Communication	Communicate the policy to all relevant internal and external parties	Specific communications/ messages/ statements/ announcements to internal and external parties about policy
						A.3.5	Interdependencies	Document the relationships and dependencies to other policies and procedures	An artefact showing the relationships/ linkages and updates to other related policies to include reference to the ISIMF (e.g. Business Continuity and Disaster Recovery procedures).
						A.3.6	Risk alignment	Document the links to the organisational risk management framework	Evidence that the ISIMF has been integrated with the organisational risk management framework
			A.4	Implementation plan	To provide the resources and a roadmap for the implementation of the ISIMF	A.4.1	Roadmap	A roadmap for maturing the incident management capability	An artefact showing the planned activities over time to mature the capability

Phase			Activity		Objective	Controls			Examples/Output
						A.4.2	Performance measures	Define performance measures and monitor the effectiveness of the ISIMF against these	An artefact defining the performance measures and evidence of actual data collection and response to collected data
						A.4.3	Executive approval	Executive approval of the plan	Meeting minutes or any other evidence showing direct (not implicit) approval of implementation plan
			A.5	Internal processes, procedures and planning	To support the policy objectives	A.5.1	Internal documentation	Document the supporting processes, procedures and incident management plan that specify the baseline of what must be done	Artefacts detailing how to achieve the policy objectives
						A.5.2	Coverage	Internal documentation supports the activities of all the information security incident management phases	An artefact defining and supporting all the information security incident management phases (i.e. plan and prepare, detect and report, assess and decide, respond, lessons learnt) Processes address coverage across the organisation
						A.5.3	Roles and responsibilities	Assign the roles and responsibilities of key stakeholders of the processes, procedures, and the incident management plan	Evidence of 'RACI model' assigning who is Responsible, Accountable, Consulted and Informed throughout the incident management processes, procedures and incident management plan including documentation governance (i.e. drafting, approvals and reviews)
						A.5.4	Prioritisation	Define how to prioritise specific information security incident categories and the processes to support the consistent application of these categories	An artefact articulating how incidents are prioritised

Phase			Activity		Objective	Controls			Examples/Output
						A.5.6	Communication	Define how and when to communicate with internal and external parties (e.g. oversight bodies, regulators, media, service providers, and other organisations)	An artefact detailing communication protocols showing who can say what and when
						A.5.7	Testing	Regularly test the incident management plan	Evidence of testing (e.g. calendar invites, test plan, outcomes of exercises)
			A.6	Resources	To provide the required tools throughout the information security incident management phases	A.6.1	Templates	Develop templates	Templates such as notification forms, post incident reports, etc.
						A.6.2	Toolkits	Identify the required tools to manage the incident (e.g. facilities, systems, and people)	Evidence of tools to support the information security incident management processes
						A.6.3	Contact lists	Compilation of contact lists of all relevant internal and external stakeholders	Contact lists showing details of every key stakeholder and secondary contact allowing 24/7 access to personnel/ services
			A.7	Roles and responsibilities	To ensure that all internal and external parties understand their roles and responsibilities	A.7.1	Team model	Define the information security incident management team model (e.g. centralised or distributed) addressing both oversight/ management and response	Details of the information security incident management team model(s), including security incident management and response
						A.7.2	Roles and functions	Define the role and function of each participant taking into account both internal and external parties	An artefact defining the role and function (e.g. RACI model of internal and external stakeholders including law enforcement, regulators, and other third parties)
						A.7.3	Authority	Define the authorities for decision making	An artefact stating the authority for decision making for any financial, reputational, operational, legal and regulatory implications

Phase			Activity		Objective	Controls			Examples/Output
						A.7.4	Consumers	Define the needs of consumers in the context of incident management	An artefact showing the information/ data needs for consumers/ customers during an information security incident (including both suppliers and recipients)
						A.7.5	Dependencies	Define the dependencies on services and resources both within and beyond the organisation (e.g. legal, IT support, regulatory, and facilities)	An artefact showing the dependencies on and by other parties/ services
			A.8	Skills, training and awareness	To ensure that all relevant parties are aware, well prepared and skilled in information security incident management	A.8.1	Skills and competencies	Select stakeholders with suitable skills, matching their roles and responsibilities in the ISIMF 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, finance, facilities, executives, records management, and ICT) Staff have completed relevant security incident training
						A.8.2	Training	Document a training plan addressing the ongoing training needs of the information security incident management team(s)	A training plan detailing the actions, activities and focus areas of those involved in information security incident management
						A.8.3	Awareness	Define and implement an information security incident awareness program ensuring all internal and external stakeholders are aware of the ISMF	Evidence of communications to internal and external stakeholders Spot-check of staff awareness of the ISMF
B	Detect and Report	The capability to identify security events	B.1	Threat intelligence	To proactively detect and report any threats and vulnerabilities	B.1.1	Threat analysis	Perform external/ internal threat analysis to establish an understanding of the threat environment and in turn detect changes	Evidence of threat analysis (e.g. threat reports, and threat & risk workshops)

Phase			Activity		Objective	Controls			Examples/Output
						B.1.2	Frequency	Perform frequent threat analysis where the frequency is defined by the business based on the organisational context as well as the criteria for unscheduled analysis activities	An artefact detailing the frequency of threat analysis including criteria for unscheduled reviews based on changes to the threat environment
						B.1.3	Quality/ reliability	Determine and include the reliability and quality of the information being analysed of the threat assessments	Threat report includes a quality/ reliability statement of the threat intelligence
			B.2	Vulnerability analysis / attack vectors	To ensure 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
			B.3	Security monitoring	To provide timely detection of events and information security incidents	B.3.1	Indicators	Define information security incident indicators and precursors	An artefact stating the precursors and information security incident indicators
						B.3.2	Event monitoring	Monitor and assess events utilising the defined indicators and precursors	Evidence that events are monitored/ assessed using the defined indicators/ precursors
						B.3.3	Testing	Test any new defined information security incident indicators or precursors against the existing security events	Evidence that retrospective review of security events was performed when information security incident indicators or precursors have changed
						B.3.4	Alerting	Document the alert thresholds for information security events (both automated and through user reporting)	A system which could include an automated tool that has a built in alert function Significant changes to a ‘factor area’ for a security clearance holder
C	Assess and Decide	The capability to assess information security events, decide on whether they are	C.1	Triage	To assess information security events and when deemed an incident,	C.1.1	An event is declared as an incident	Assessments are undertaken to determine whether to categorise an event as an information security incident	Internal report or briefing

Phase			Activity		Objective	Controls			Examples/Output
		information security incidents and perform analysis activities			determine how to best manage them	C.1.2	Process	Consider the characteristics of the information security incident and follow pre-defined response and management processes	Evidence of following the process
						C.1.3	Timeliness	Assess information security incidents in a timely manner (ensuring 24/7 response where required)	Process review showing that reported information security incidents are assessed and addressed within a reasonable timeframe
						C.1.4	Parameters/ scope	Establish a terms of reference for the information security incident including response parameters (where required)	Terms of reference artefact for a particular information security incident
						C.1.5	Register	Record all reported information security incidents	A register showing recorded incidents and accompanying assessment outcomes
						C.1.6	Prioritisation	Prioritise all information security incidents according to relevant internal documentation	A record of the priority assessment is captured in the information security incident register
						C.1.7	Categorisation	Categorise all recorded information security incidents	A record of the category is captured in the information security incident register
						C.1.8	Asset owners	Identify asset owners during the triage assessment (if applicable)	A record of the asset owner(s) is captured
			C.2	Analysis	To analyse information security incidents as information becomes available	C.2.1	Subject Matter Expert (**SME**) engagement	Engage suitable SMEs from relevant areas and bring these SMEs into the information security incident response process	An artefact showing how SMEs are engaged
						C.2.2	Business impacts	Business impacts resulting from the information security incident are assessed	An artefact showing that business impacts are assessed

Phase			Activity		Objective	Controls			Examples/Output
						C.2.3	Ongoing analysis	As additional information becomes available, the original assessment is re-considered to identify whether the information security incident needs to be re-prioritised or response activities adjusted	Evidence from past incidents showing risks 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 protocols according to the information security incident characteristics	Evidence that information flows are controlled and pre-defined (who can talk to whom and when) during the response phase
D	Respond	The capability to respond to information security incidents	D.1	Investigation decision and handover	To ensure appropriate incident response activities	D.1.1	Investigation handover	Determine whether the incident needs specific investigation response and where required, handover to the appropriate authorities to undertake their duties	Referrals to law enforcement Decisions to change an administrative incident to criminal incident
			D.2	Containment	To prevent further damage from the information security incident in a controlled fashion	D.2.1	Containment strategies	Follow pre-defined containment strategies set out under internal processes	Evidence that documented containment strategies have been followed (e.g. wipe and restore, and monitor and observe) Evidence that consideration has been given to the broader information security issues such as forensics, personnel security, disaster recovery, business continuity management, etc.
						D.2.2	Authority	Follow pre-defined decision authorities for the containment of the information security incident	Evidence that the documented decision authorities for the containment strategy have been followed
			D.3	Gather evidence	To provide assurance of no tampering with evidence	D.3.1	Evidence collection	Gather, record and maintain a chain of custody of evidence related to the incident	Log/ activity book Tagged and sealed artefacts

Phase			Activity		Objective	Controls			Examples/Output
			D.4	Eradicate	To address issues leading to the information security incident	D.4.1	Controls	Define a process and implement supporting controls to rectify any issues and control(s) that failed to prevent the information security incident	Implementing and mitigating control(s)
						D.4.2	Scope of rectification	Rectification has considered areas that are not impacted but rely on the same controls	A process showing that after control failures, similar controls or controls in other areas are reviewed Evidence from past events showing that such review is performed
			D.5	Recover	To recover from the information security incident and resume normal business operations	D.5.1	Business continuity	Initiate Business Continuity Plan (**BCP**)	Evidence of linkage to business continuity management
						D.5.2	Recovery strategies	Follow pre-defined restore strategies outlined in internal processes	Evidence of following the recovery strategies
			D.6	Communication / engagement	To provide accurate, factual and timely information to stakeholders	D.6.1	Communication/ engagement plan	Follow pre-defined communications and/ or an engagement plan that identifies who has the authority to communicate to different stakeholders	An engagement/ communication plan Communication to relevant stakeholders/ affected parties Notification to regulator(s) A statement of authority covering all identified receivers of communication
						D.6.2	Frequency	Provide frequent status updates to key stakeholders	Evidence that key stakeholders have been updated on the status of information security incidents
			D.7	Resolution and closure	To ensure timely closure of incidents and maintain complete and accurate records	D.7.1	Incident closure	Confirmation that the incident has been satisfactorily addressed and no further action required	Report or briefing to relevant stakeholders
						D.7.2	Recordkeeping	Update the incident register with incident closure details	Incident register

Phase			Activity		Objective	Controls			Examples/Output
E	Lessons Learnt	The capability to reduce the business impact of an information security incident, prevent incidents from re-occurring and improve information security incident management	E.1	Post incident review	To provide direct feedback on the effectiveness of information security incident management	E.1.1	Review	Perform a subjective and objective assessment of the ISIMF	Evidence that a review has occurred after an information security incident
			E.2	Record incident insights	To support the ongoing improvement of the information security incident response capability	E.2.1	Outcomes and recommendations	Record the outcomes and recommendations of the information security incident	An information security incident register containing performance metrics such as categorisation, business impact, time per incident, review outcomes, recommendations, links to risk register, etc.
			E.3	Awareness	To ensure that all relevant stakeholders are aware of any updates to the ISIMF	E.3.1	Response resources	All stakeholders with an identified role in the ISIMF have been made aware of the framework and any changes to it	Evidence of communications to staff about changes to the incident management processes, roles/ responsibilities or response resources
			E.4	Information sharing	To ensure that all relevant stakeholders are provided relevant information about the information security incident	E.4.1	Information exchange	Follow the pre-defined process that identifies the stakeholders not directly involved during the response phase	Evidence of information sharing (e.g. engagement with ACSC, AFP, AusCERT, idcare, other linked agencies, and regulators)
			E.5	Evidence retention	To ensure evidence relating to the information security incident is retained in a suitable manner (if required)	E.5.1	Retention and preservation	Define any retention and preservation of evidence relating to the information security incident including any legal and regulatory requirements	An artefact defining retention/ preservation requirements of evidence
			E.6	Audit and reviews	To ensure the ongoing effectiveness of the ISIMF	E.6.1	Scope	Define the scope for audits and reviews of the ISIMF	A definition of audit scope
						E.6.2	Coverage	Audit and reviews cover all aspects of the ISIMF	Evidence of audit activities across components of the ISIMF

Phase			Activity		Objective	Controls			Examples/Output
						E.6.3	Linkage to threats/ risks	Audit and reviews of the ISMF take into account existing risks and threats	Audit planning considers incidents, threats and risks
						E.6.4	Frequency	Define the frequency for audit and reviews of the ISIMF (i.e. conducted on a regular basis or if significant events have occurred)	An artefact stating the frequency for audit/ reviews, taking into account the need for unscheduled reviews to respond to significant incidents
			E.7	Continuous improvement	To ensure the ISIMF is continuously reviewed, validated and updated	E.7.1	Framework review	Review the effectiveness of the ISIMF and the Incident Response Team (**IRT**)	Review activities since the last recorded information security incident
						E.7.2	Policy review	Review the policy in line with the organisation’s policy governance framework In absence of such a framework, the review is done at least annually	An audit trail for policy review (e.g. email, agenda items, and versioning records)
						E.7.3	Process, procedures and plan review	Review the processes, procedures and incident management plan 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, and revision history)