MOBIUS INCIDENT MANAGEMENT: A FOCUS ON INFORMATION SECURITY AND PRIVACY INCIDENTS

The need for appropriate management of information security and privacy incidents ("incidents") has not been clearly articulated in organisations, leading to inability to identify and manage incidents as effectively as possible. In most instances, this is managed in two ways:

- As part of the broader incident management process where a clear differentiation between information security incidents and operational IT incidents are not defined; or
- At low level of maturity without the necessary policy, process and supporting documentation required to implement an effective information security and privacy incident management function.

It is essential for any organisation with a key focus on information security and privacy, to have a specialised, structured and tested approach to the management of incidents of this complex nature. Without this specialised focus, organisations may find themselves managing incidents in a way that is inadequate and misaligned with information security and privacy requirements. This in turn may result in ineffective business operations, legal and/or regulatory implications and financial consequences. Although the management of incidents should be specialised, it is vital that this addition of incident management aligns to the operational IT incident management process as well as the business continuity requirements of the organisation.

INTEGRATING INFORMATION SECURITY AND PRIVACY INCIDENT MANAGEMENT WITHIN YOUR ORGANISATION

Mobius recognises the need for alignment of this specialised form of incident management to existing processes within the organisation and has defined a lifecycle that caters to this need. Within this lifecycle a defined set of steps, specific to the management of information security and privacy incidents (refer to figure 1), as well as the documentation required to support these steps have been defined.

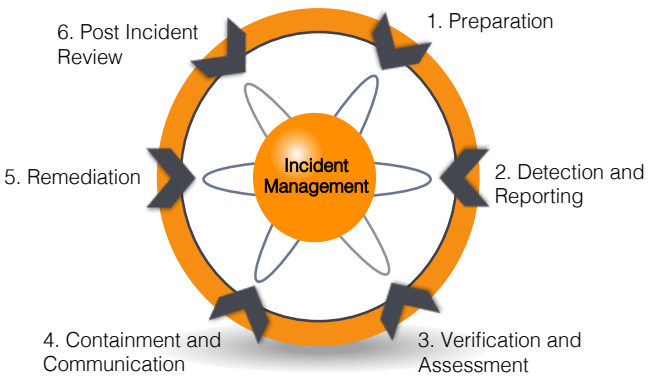

Figure 1: Information Security and Privacy Incident Management Lifecycle

INCIDENT MANAGEMENT LIFECYCLE DEFINED

Phase	Description	Differentiation to IT Operational Incident Management	Supporting documentation
Preparation	This step includes the identification of common information security and privacy incidents and includes the development of incident scenarios along with supporting documents needed to implement phases of the lifecycle. Further a key outcome of this phase is identification of roles and responsibilities for each scenario.	Due to the various number of IT operational incidents preparation is usually not a key focus area. In cases where this step is in place, scenarios to address common incidents are not defined or documented.	• Incident Management Policy • Incident Management Guideline • Incident Management Process • RACI Model
Detection and reporting	This step includes defining the mechanisms required to detect incidents and the means through which incidents are reported.	Detection mechanisms used for information security and privacy incidents differ from the detection mechanisms used for IT operational incidents due to its focus on security and information. In addition, the ways in which these incidents are reported differ due to their sensitive nature.	• Incident Classification Guide • Incident Management Repository • Incident Tracking Report
Verification	This step includes examination of the reported incident during which the incident is validated. This is needed to prevent unnecessary work or reporting to board and executives where reported incidents are in fact not material.	None	• Incident Categorisation Guide • Incident Management Repository • Incident Tracking Report
Assessment	This step includes assessment of the urgency and impact of the incident to determine the incident priority as well as the cause of the incident.	Assessment of information security and privacy incidents includes determining the classification of the information affected and to what level this is affected as well as the impact on the confidentiality, integrity and availability of the information.	• Impact and severity checklist • Incident Management Repository • Incident Tracking Report
Containment	This step includes the identification of containment measures that may be implemented in order to reduce the extent and impact of the incident.	Due to the nature of information security and privacy incidents, impacts and consequences of the incident are far greater than those of IT operational incidents. Therefore the lifecycle includes a step for containing the incident.	• Incident Management Repository • Incident Tracking Report
Remediation and closure	This step includes remediation of the incident and recovery of affected systems and affected information.	During remediation of incidents, where it has been established that personal or sensitive information was breached; reporting of this may be required to the affected parties, relevant regulatory bodies and law enforcement.	• Incident Management Repository • Incident Tracking Report
Post incident review	The step includes a review of incidents to identify improvement areas once the incidents have been remediated and closed	Where security and privacy environments are more mature, board and executive expect effective reporting to be done on a regular basis regarding incidents, breaches, their impact on the business and remedial actions.	• Post incident review checklist