Company Logo

Info-Tech Research Group
Security, Risk & Compliance

Security Incident Management Runbook: Malicious Email

Last revised: MM/DD/YY

Contents

Revision History

Version	Change	Author(s)	Date of Change
1.0	Initial Draft		

Introduction

Effective and efficient incident management involves a formal process to detect, analyze, contain, eradicate, recover, and conduct post-incident activities. This runbook provides detailed procedures that govern the incident response procedure to handle **malicious email incidents.**

Incident Assessment Methodology

The incident assessment methodology consists of the evaluation of *impact, scope,* and *threat escalation.*

Impact

Evaluate the effects of malicious emails on business functions, data, and recovery efforts. Incident impact should be categorized based on the factors below: [To be completed by and catered to the member organization. Below is an example.]

1. The current and future functional impact on any business functions or operations.
2. The informational impact as it relates to the confidentiality, integrity, and availability of the organization's data.
3. The time and required resources needed to recover from the incident.

Malicious Email Impact Criteria	
Rating	Definition
High	Malicious email was sent and delivered, and the end user interacted with hostile content (opened the email) and performed further actions (e.g. user entered credentials or transferred funds). The email looks authentic (and therefore, may trick others).
Medium	Malicious email was sent and delivered, and the end user interacted with the hostile content (opened the email), but did not perform further actions (e.g. user did not enter credentials). The email looks authentic.
Low	Malicious email was sent and delivered to an end user, but the user did not interact with the hostile content/open the email. The email may or may not look authentic.

Scope

Evaluate the scope (i.e. breadth/magnitude) of the incident on systems, users, endpoints, etc. Incident scope is a critical component that aids in decision making throughout the incident management process. [To be completed by and catered to the member organization. Below is an example.]

Malicious Email Scope Criteria	
Rating	Definition
High	>99 active email accounts were targeted OR 1 or more executives/privileged accounts were targeted.
Medium	11-99 active email accounts were targeted OR confirmed spear phishing event.
Low	<11 active email accounts were targeted.

Threat Escalation Protocol

A threat escalation protocol is used to define the type of stakeholders needed during the incident management process. Informing and consulting these stakeholders during the incident management process is crucial when defending the organization against malicious emails. A threat escalation protocol clearly defines escalation procedures for malicious email incidents. [To be completed by and catered to the member organization. Below is an example.]

Incident Management Overview

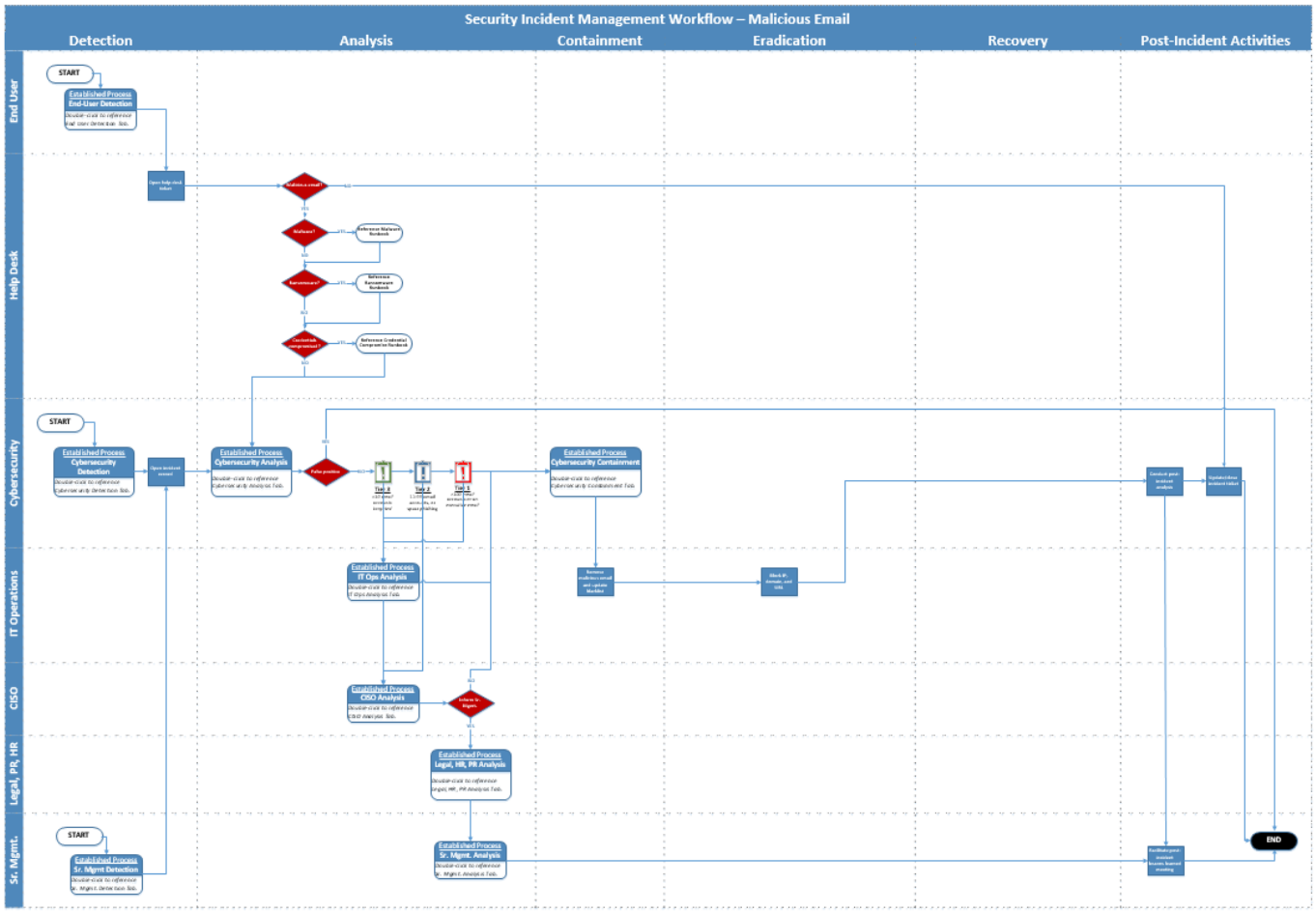
The table below includes the definition of malicious emails, the effects of phishing on your organization, and a summary of the response required to deal with this incident.

Malicious Email	The use of emails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website or opening a malicious file. For example, the email and the website look like they belong to a bank that the user does business with or it may have malware attached. In these case, other runbooks may need to be initiated (e.g. malware, compromised credential, ransomware).
What Is the Incident?	Incidents could include whaling, phishing, spear phishing, or spam. **Phishing:** The use of emails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically, the email and the website look like they belong to a trusted organization that the user does business with. **Whaling:** The use of emails that appear to originate from a trusted source to trick a **senior executive** into entering valid credentials at a fake website, clicking a malicious link, opening a malicious file, wiring unauthorized funds, or providing sensitive/corporate data. **Ransom Demand/Scam:** The use of emails from a suspicious source to demand a ransom or solicit participation in a scam, such as lottery scams, auto-auction, or disaster relief. **Spear Phishing:** The use of emails that appear to originate from a trusted source to trick a **targeted user/group** into entering valid credentials at a fake website, clicking a malicious link, opening a malicious file, or providing sensitive/corporate data. **Spam:** The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
Why Should We Care?	Email is a common attack vector, leveraged by threat actors to carry out their cyber-threat campaigns. Since many employees have a user account with email, it is a frequently used attack type.

How Do We Respond?	During malicious email incidents, stakeholders defined in the threat escalation protocol work collaboratively throughout the entire incident management process. Major activities that take place during malicious email incidents include the following: 1. **End Users:** Report suspicious incidents and provide any support to help desk and cybersecurity staff. 2. **Help Desk:** Interact directly with the end user to gather incident-related information, create and update tickets, and coordinate with the end user throughout the incident management process. 3. **Cybersecurity:** Monitor security events, analyze logs, conduct open-source intelligence research, provide technical support, identify any control weaknesses, coordinate all incident activities, and document root cause and investigative activities in an incident record. 4. **IT Operations:** Monitor email server events, analyze email server logs, conduct open source intelligence research, remove any infected email servers from the network, and restore impacted data. 5. **CISO:** Notify and coordinate with the relevant stakeholders and senior management, evaluate control weaknesses, update policies, and facilitate any post-incident activities. 6. **Legal, HR, PR:** Evaluate any brand/reputational damage, determine regulatory compliance violations, conduct any employee disciplinary actions, and facilitate any external reporting. 7. **Senior Management:** Approve any proposed control strategy and allocate budget or resources. 8. **External Third Parties:** Provide incident investigative support and sharing information.

Incident Management Workflow: Malicious Email

The workflow diagram below outlines the incident management process from detection to post-incident activities, including the responsibilities of each stakeholder in each phase. The workflow outlines the decisions, actions, and pre-established processes that are required to deal with the incident at each stage, for all three threat magnitudes.



Response Procedures

The actions required to deal with malicious email are detailed below for each relevant stakeholder (team), in each of the six phases (detection, analysis, containment, eradication, recovery, and post-incident).

Detection Phase

During the detection phase, teams will evaluate a potential malicious email incident, for example, a phishing or whaling attempt. Once an incident has been detected, a help desk ticket or incident record/ticket is opened to initiate the detection phase.

Team	Description	Questions	Action
Detection: End User	During the detection phase, the end user will report a potentially malicious email.	• Does this email seem suspicious? • Do I recognize the sender? • Is the request abnormal?	☐ The user reports a suspected malicious email.
Detection: Help Desk	During the detection phase, help desk staff will monitor calls and submitted tickets.	• Are any end users reporting a potentially malicious email?	☐ Open a help desk ticket. ☐ Determine if incident needs to be escalated to other stakeholders. Begin analysis phase. ☐ Maintain communications with any impacted end users.
Detection: Cybersecurity	During the detection phase, cybersecurity staff monitor email gateway and other **events,** and open incident records as appropriate.	• Are malicious emails being caught by the email gateway? • Are external email IOCs targeting the organization?	☐ Compare externally gathered IOCs to email security gateway logs. ☐ Monitor the email security gateway for suspicious events. ☐ Review and monitor other events and alerts, including the following: ○ SIEM ○ Firewall ○ IDS/IPS ○ Web proxy connections ○ Antivirus ○ Anti-malware ☐ Open an incident record (if not opened yet).
Detection: IT Operations	During the detection phase, IT operations staff monitor email server logs (Exchange, SMTP, Send Mail, etc.) and other **events,** and escalate **incidents** to the cybersecurity team.	• Are there indications of malicious email sent to the email server?	☐ Review and monitor email server logs. ☐ Compare externally gathered IOCs to email server logs. ☐ Escalate incident to Cybersecurity.
Detection: CISO	No incident management responsibilities.		
Detection: Legal, HR, PR	No incident management responsibilities.		
Detection: Senior Management	During the detection phase, senior management staff will	• Have I received any suspicious emails?	☐ Report suspected whaling email to help desk.

	notify and escalate any suspicious malicious emails (whaling or spear phishing).	• Am I being targeted for an abnormal request? • Is there an unexpected attachment?	

Analysis Phase

During the analysis phase, teams will analyze the incident to determine the impact of the threat. Depending on the impact, a number of teams will be involved in the remediation of the malicious email incident, and the notification of the threat will be escalated as appropriate.

Team	Description	Questions	Action
Analysis: End User	During the analysis phase, end users will provide information related to the incident as required.	• What are the events that led to this suspected incident? • Did I interact with the email content? • Did I input credentials? • Did I open an unknown attachment?	☐ Provide information related to the incident to the help desk.
Analysis: Help Desk	During the analysis phase, help desk staff directly interact with the end user, ask incident-related questions, take actions, and document findings in the help desk ticket.	• Did the end user click a hyperlink? • Did the end user open a file attachment? • Did the end user enter credentials? • Did the end user visit a suspicious website? • How many users received the email? • Was an executive targeted?	☐ Perform preliminary analysis to understand what happened: the nature of the incident, the impact, and the scope. ☐ Validate the legitimacy of the suspicious email. ☐ Update help desk ticket, documenting all answered to incident-related questions. ☐ Search ticketing platform to identify other impacted end users. If multiple end users are impacted, create a parent/child ticket. ☐ If there are indications that a privileged account has been successfully targeted escalate **immediately** to cybersecurity team. ☐ Maintain communications with any impacted users.
Analysis: Cybersecurity	During the analysis phase, cybersecurity staff will analyze appropriate logs, conduct open-source intelligence research, provide technical support, provide incident coordination support, directly interact with the end user, ask incident-related questions, take actions, and document findings in the incident record.	• Did the end user click a hyperlink? • Did the end user open a file attachment? • Did the end user enter credentials? • Did the end user visit a suspicious website? • Are any locally stored, suspicious file extensions identified? • Is the end user being targeted in a spam, phishing, spear phishing, or whaling campaign?	☐ Gather answers to incident-related questions. ☐ Search web proxy logs to identify any outbound command and control traffic. ☐ Conduct open-source threat intelligence analysis to identify comparative indicators of compromise (IOCs). ☐ Analyze email gateway and system and server logs. ☐ Determine if any end-user devices were compromised. ☐ Review an endpoint protection event or series of events.

		• Are there indications that a crime was committed (e.g. ransom demand)?	☐ If the end user is being targeted in a spam campaign, recommend a review of spam-filtering rules. ☐ If the end user is being targeted in a phishing or spear-phishing campaign, then determine if any user credentials were compromised. If so, initiate the credential compromised runbook. ☐ If the end user is being targeted in a phishing or spear phishing campaign, then determine if the end user clicked on a malicious hyperlink or opened a weaponized file attachment. If so, initiate the malware or ransomware runbook. ☐ If the end user is being targeted in a whaling campaign, determine which senior executives were targeted. Communicate accordingly.
Analysis: IT Operations	During the analysis phase, IT operations staff will analyze the ability for a repetitive attack of the same nature to occur.	• Are the secure email gateway controls effective to prevent future attacks? • Can the malicious emails be removed from the end user's inbox? • Can any IPs, email addresses, URLs, and domains be blocked at the web proxy?	☐ Determine if there are any malicious emails in the end user's inbox. ☐ Identify any malicious email server IPs and email addresses. ☐ Identify any malicious domains and URLs at the web proxy.
Analysis: CISO	During the analysis phase, the CISO will notify and coordinate with the relevant stakeholders and senior management.	• Was an executive targeted (i.e. whaling/spear-phishing)?	☐ Publish corporate-wide situational awareness alerts to inform end users of major phishing attempts. ☐ Coordinate and inform senior management of any incident updates, if whaling. ☐ Report any external criminal activities to senior management.
Analysis: Legal, HR, PR	During the analysis phase, legal, HR, and PR staff will analyze any insider activity, legal requirements, and brand/reputational damage.	• Are there potential legal repercussions to the incident? • Was there any insider activity or other misuse of credentials? • Was there any brand or reputational damage?	Legal: ☐ Determine if any regulatory, legal, or compliance mandates have been violated or impacted. ☐ Determine if any breach notifications are required. ☐ Begin process to notify required parties. HR: ☐ Determine if any employee acceptable-use or security policies have been violated. ☐ Determine if any preliminary employee disciplinary actions are required immediately. PR:

			☐ Determine if any public reputational or brand damage has occurred. If so, begin process/campaign to address it.
Analysis: Senior Management	During the analysis phase, senior management staff will notify and coordinate with the relevant stakeholder.	• Is there any brand/reputational damage? • Have we been informed of any crimes? • Is there any major business disruptions?	☐ Provide an incident summary and updates to the board of directors/stakeholders. ☐ Approve reporting crime to law enforcement, if necessary. ☐ Analyze and approve emergency budget, resource, or control requests, as appropriate. ☐ Approve communication of incident information with external parties.
External	No incident management responsibilities.		

Containment Phase

During the containment phase, teams will isolate and contain any malicious emails.

Team	Description	Questions	Action
Containment: End User	No containment responsibilities beyond ongoing cooperation with incident responders.		
Containment: Help Desk	During the containment phase the help desk will maintain communications with any impacted end users.	• Do any end users need to be notified?	☐ Maintain communications with any impacted end users.
Containment: Cybersecurity	During the incident management containment phase, cybersecurity staff will document all findings in the incident report and identify any additional compromised email accounts.	• Which stakeholders need to be notified of the incident report findings? • Are there any other compromised email accounts? • How can we prevent any future targeted malicious email campaigns?	☐ Provide incident coordination support. ☐ If the end user is being targeted in a spam campaign, review spam filtering rules. ☐ If the end user is being targeted in a phishing campaign, then reissue any user credentials that were compromised and investigate any malicious hyperlinks or opened weaponized file attachments.
Containment: IT Operations	During the containment phase, the IT operations staff will remove the ability for a repetitive attack of the same nature to occur.	• Are the secure email gateway controls effective to prevent future attacks?	☐ Remove malicious email from end user's inbox. ☐ Block any malicious email server IPs and email addresses. ☐ Update any blacklists. ☐ Block malicious domains and URLs at the web proxy.
Containment: CISO	No containment responsibilities beyond ongoing communication		

	and updates with stakeholders.		
Containment: Legal, HR, PR	During the containment phase, the legal, HR, and PR staff will evaluate if any legal actions need to be taken.	• Are there any legal requirements or notification requirements?	Legal: ☐ Continue legal actions as necessary, informing affected parties as required by regulations. PR: ☐ If necessary, address the affected stakeholders (including the public), informing them of the steps that have been taken to contain the incident and future steps to fully remediate the incident. HR: ☐ Continue HR actions, as necessary, particularly containing any further employee misuse or violations.
Containment: Senior Management	No incident management responsibilities.		

Eradication Phase

During the malicious-email incident-management eradication phase, teams will restore and reissue endpoints and servers.

Team	Description	Questions	Action
Eradication: End User	No incident management responsibilities.		
Eradication: Help Desk	During the eradication phase, the help desk staff will maintain communications with impacted end users.	• Does the end user need to be notified?	☐ Maintain communications with any impacted end users.
Eradication: Cybersecurity	During the eradication phase, cybersecurity staff will work to eliminate the root cause of the incident.	• Did anyone else receive the malicious email? • Has the malicious email campaign ended?	☐ Review email logs to determine if any other users are being targeted in the malicious email campaign. ☐ Determine if any other similar malicious email campaigns have been initiated.
Eradication: IT Operations	During the eradication phase, IT operations staff will remove the ability for a repetitive attack of the same nature to occur.	• How can we prevent future attempts from this malicious email campaign?	☐ Block IP and email address. ☐ Remove malicious email from end user's inbox. ☐ Block domain and URL.
Eradication: CISO	During the eradication phase, the CISO will develop any emergency plans and approve additional resources.	• Do any new controls need to be implemented? • Do any controls need to be updated?	☐ Approve additional controls and resources to eliminate the root cause of the incident, as necessary. ☐ Develop any emergency/disaster recovery plans, as appropriate.

		• Do any policies need to be updated?	☐ If in violation of acceptable use policy, approve any disciplinary actions as appropriate.
Eradication: Legal, HR, PR	No specific eradication responsibilities beyond on going processes already established.		
Eradication: Senior Management	No specific eradication responsibilities beyond ongoing support and approval, as necessary.		

Recovery Phase

During the recovery phase, teams will enact process and procedures for recovery and full restoration of any infected endpoints or servers during the incident. End users will be informed when operations are back to normal and all affected credentials will be reissues, if not already.

Team	Description	Questions	Action
Recovery: End User	No incident management responsibilities.		

Recovery: Help Desk	During the recovery phase, the help desk will maintain communications and coordinate recovery with affected end users.	• Does the end user need to be notified? What do they need to know?
		• Is the ticket up-to-date?
			☐ Maintain communications with any impacted end users. Inform users:
			  ○ When operations are back to normal.
			  ○ Of any required changes (e.g. updates to systems, passwords).
			  ○ Of updated training and awareness material regarding the incident.
			☐ Re-issue end-user devices and credentials, if not already complete.
			☐ Ensure ticket is updated with all relevant information.

Recovery: Cybersecurity	During the recovery phase, cybersecurity staff will document any findings in a root-cause incident report.	• Is the incident report comprehensive enough? • Has a root cause been determined and documented?	☐ Complete the root-cause incident report. ☐ Ensure incident record/ticket is updated with relevant information. ☐ Advise the CISO of any controls, processes, or policies that need to be updated.
Recovery: IT Operations	During the recovery phase, the IT operations staff will provide input to the root-cause incident report and restore systems.	• What needs to be contributed to the root-cause incident report?	☐ Provide any IT operations input for the root-cause incident report. ☐ Restore any systems and/or data, if affected. ☐ Once restored, validate and test that all systems/data/functionality have returned to normal operations.

Recovery: CISO	During the recovery phase, the CISO will evaluate any weaknesses in security controls or policies as appropriate.	• Do any controls or policies need to be updated?	☐ Review any security policies or controls, as appropriate. ☐ Inform senior management that operations have been restored.
Recovery: Legal, HR, PR	During the recovery phase, legal, HR and PR staff will determine if all relevant processes are complete.	• Is IT input required for the continuation and completion of ongoing Legal, HR, or PR processes?	☐ Legal: Follow-up with any legal implications and requirements. ☐ HR: Ensure employee records are updated with any infractions (e.g. misuse of corporate resources causing an incident) and subsequent disciplinary actions. If disciplinary actions have not been issued yet, begin process in coordination with the employee's manager. ☐ PR: Communicate with stakeholders/public that the incident has been resolved, including next steps.
Recovery: Senior Management	No incident management responsibilities.		

Post-Incident Phase

During the post-incident phase, teams will perform root-cause analysis and lessons-learned activities with various teams and stakeholders within the organization. Any recommended outcomes should be implemented to ensure continuous improvement, and all related active tickets should be updated and closed. This phase involves performing post-mortem, root-cause analysis, and lessons-learned activities with various teams and stakeholders within the organization.

Team	Description	Questions	Action
Post-Incident: End User	During the post-incident phase, affected users may provide additional details for post-incident meetings/reports and may participate in additional awareness and training.	• How was my credential compromised? • What should I do next time?	☐ If necessary, a primary affected user may answer questions regarding the source of the incident. ☐ General end users may participate in updated awareness and training as a result of the incident.
Post-Incident: Help Desk	During the post-incident phase, the help desk may participate in post-incident meetings, as necessary.	• Are there any help desk processes that need to be improved?	☐ Participate in post-mortem/lessons-learned meetings, as necessary.
Post-Incident: MSSP/Security Operations	During the post-incident phase, the MSSP/security	• Are there any MSSP/security operations processes	☐ Participate in post-mortem/lessons-learned meetings, as necessary.

	operations staff will support any post-incident activities, as appropriate.	that need to be improved?	
Post-Incident: Cybersecurity	During the post-incident phase, cybersecurity staff will support any post-incident analysis and ensure all findings are documented in an incident report.	• What happened? • How did we respond? • What should we do next time? • Are there any cybersecurity processes that need to be improved?	☐ Participate in post-mortem/lessons-learned meetings, as necessary. ☐ Update and close incident ticket. ☐ Provide awareness and training reminder to users of proper password practices.
Post-Incident: IT Operations	During the incident management post-incident phase, IT operations staff will support any post-incident activities, as appropriate.	• Are there any IT operations processes that need to be improved?	☐ Participate in any post-mortem/lessons-learned meetings, as appropriate.
Post-Incident: CISO	During the incident management post-incident phase, the CISO will facilitate any post-incident activities.	• How can the incident response process be improved?	☐ Conduct and facilitate any post-mortem/lessons-learned activities. ☐ Facilitate post-mortem/lessons-learned meeting.
Post-Incident: Legal, HR, PR	During the incident management post-incident phase, legal, HR, and PR staff will support any post-incident activities, as appropriate.	• Are there any legal, HR, or PR processes that need to be improved?	☐ Participate in any post-mortem/lessons-learned meetings, as appropriate. ☐ If new findings become known as a result of post-incident activities, follow up with any new or ongoing legal, HR, and PR duties that have not already been addressed. ○ Legal: Follow up with any legal actions, if required. ○ HR: Follow up with any employee disciplinary action, if required. ○ PR: Follow up on public and internal communications to address the resolution of the incident and steps being taken to prevent reoccurrences.
Post-Incident: Senior Management	During the incident management post-incident phase, senior management will support any post-incident activities, as appropriate.	• Are there any senior management processes that need to be improved?	☐ Participate in any post-mortem/lessons-learned meetings, as appropriate.
Post-Incident: External	No incident management responsibilities.		

For acceptable use of this template, refer to Info-Tech's Terms of Use. These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.