

ARO Critical Security Incident Response Procedure - Customer

(ISO 27001:2022 Organisational Controls, Clause 5.24)

Author	Greg Nott
Version	5.0
Date Created	26/09/2023
Last Update Date	21/10/2025
Document Control	Released
Document ID	230926-SEC-PRO-AROCriticalSecurityIncidentResponseCustomer-V5
Security Classification	Public

Table of Contents

Approval.....	4
Review.....	4
Change History.....	4
Associated Documents.....	4
Scope.....	6
Purpose.....	6
Procedure.....	6
Detection Phase.....	6
D1. Possible Security Incident Detected.....	6
D2. Incident Assessment.....	7
D3. Register Incident Ticket in ITSM.....	6
D4. Conduct Triage.....	7
D5. Assign Classification.....	7
D6. Assign Severity.....	8
D7. Assign Priority.....	8
D8. Resolve using BAU Process.....	8
D9. Mobilise CSIRT.....	9
D10. Collect Incident Data.....	9
D11. Determine Scope.....	9
D12. Identify if Incident Impacts Personally Identifiable Information (PII).....	10
D13. Data Breach Response Process.....	10
D14. Security Incident Response Process.....	10
D15. Reassess Incident.....	10
D16. Determine if Notification is Required.....	11
D17. Determine Notification Communications.....	11
D18. Notify Relevant Parties.....	11
Containment Phase.....	11
C1. Communicate to Stakeholders.....	11
C2. Develop Containment Plan.....	12
C3. Execute Containment Plan.....	12
C4. Assess Containment Measures.....	12
C5. Update Ticket in ITSM.....	12
Eradication Phase.....	13
E1. Communicate to Stakeholders.....	13

E2. Develop Eradication Plan	13
E3. Execute Eradication Plan	13
E4. Assess Eradication Measures	13
E5. Update Ticket in ITSM	14
Recovery Phase	14
R1. Communicate to Stakeholders	14
R2. Develop Recovery Plan	14
R3. Execute Recovery Plan	14
R4. Assess Recovery Measures	14
R5. Update Ticket in ITSM	15
R6. Communicate to Stakeholders	15
Post-Incident Review and Closure.....	15
P1. Conduct RCA (Root Cause Analysis)	15
P2. Document Findings	15
P3. Assign Action Owners	15
P4. Update Controls & Policies.....	16
P5. Demobilise CSIRT	16
P6. Close Ticket	16
X. End Process	16
Deviation	16
Maintenance & Testing	17
APPENDIX A: Incident Classifications	18
APPENDIX B: Incident Severity & Priority Assignment.....	19
APPENDIX C: Incident Priority SLA	20
APPENDIX D: Incident Response Process Map.....	21
APPENDIX E: Responsibility Matrix	22

Approval

Author	Issue	Approved By	Date
Greg Nott	1.0	Wayne James	07-Nov-23
Greg Nott	2.0	Wayne James	8-Jun-24
Greg Nott	3.0	Wayne James	15-Jul-24
Greg Nott	4.0	Greg Nott	10-Mar-25
Greg Nott	5.0	Greg Nott	21-Oct-25

Review

Reviewer	Review Criteria	Issue	Date
Paul Langan	ISO 27001:2022	1.0	28-Sep-23
Paul Langan	ISO 27001:2022	2.0	7-Jun-24
Paul Langan	ISO 27001:2022	3.0	15-Jul-24
Paul Langan	ISO 27001:2022	4.0	10-Mar-25
Greg Nott	Annual Review	5.0	21-Oct-25

Change History

Author	Change	Issue	Date
Greg Nott	Creation	1.0	26-Sep-23
Greg Nott	Updated references & branding	2.0	7-Jun-24
Greg Nott	BOLT adaptation	3.0	15-Jul-24
Greg Nott	Changes to responsibilities	4.0	10-Mar-25

Associated Documents

Document	Version
ITSM Process Guide	1.0

Scope

This document is part of the Integrated Management System (IMS) for ARO and is consistent with the standards listed below and describes the ARO Critical Security Incident Response Plan - Customer adopted by ARO.

- ISO 27001:2022 – Information Security Management Systems
 - ISO 27017:2015 – Code of Practice for Cloud Services
 - ISO 27018:2020 – Code of Practice of Personally Identifiable Information (PII)
- ISO 9001:2015 – Quality Management System
- DSPT (Data Security and Protection Toolkit) for the NHS.
- Cyber Essentials Plus

Purpose

This procedure describes how to respond to a critical security incident related to customer assets that are supported by ARO under an appropriate support contract.

Procedure

A simplified map of this process is available at Appendix D with responsibilities described throughout the process summarised at Appendix E.

Detection Phase

D1. Possible Security Incident Detected

Responsible: Service Desk

Support: N/A

Description: Possible Security Incidents may be detected proactively through the monitoring of security information and event management (SIEM) tools, or other system alerts. Possible incidents may also be notified to the Service Desk through customer feedback of suspicious behaviour or activity observed on customer assets. Possible incidents may be raised immediately within the ITSM such as integrated alerts or when raised directly into the ITSM portal by the reporter.

D2. Register Incident Ticket in ITSM

Responsible: Service Desk

Support: N/A

Description: Full registration of the possible incident must be completed in the ITSM to ensure that all relevant details are documented: create new ticket if needed or enrich existing ticket content including the suspected incident type, detection timestamp and any other salient information. The member of the Service Desk working the ticket assumes the role of Incident Owner. Ticket should be escalated to a Senior Responder to determine if an incident does exist that requires further investigation. Up-to-date Senior Responders are identified in the BOLT work

instruction 'Security Cases: How to Escalate for Assessment' and BOLT 'Security Incident Response' assignment group.

NB: The Incident Owner may also assume the role of Senior Responder if **EITHER:** they are already named in the 'Security Incident Response' assignment group **OR** they are experienced / competent to assess security incidents as described in this document.

D3. Incident Assessment

Responsible: Senior Responder

Support: Incident Owner

Description: The Senior Responder must assess whether the detected event constitutes a security incident based on predefined criteria, such as indicators of compromise (IoCs), unusual behaviour, or known attack patterns. Incident Assessment & Triage is to be conducted per the SLA's in Appendix A, based on the initial alert priority where one exists.

- Security Incident Confirmed: Continue procedure at D4
- No Incident Confirmed: Close Ticket at P6.

NB: The Incident Owner may also assume the role of Senior Responder if **EITHER:** they are already named in the 'Security Incident Response' assignment group **OR** they are experienced / competent to assess security incidents as described in this document.

D4. Conduct Triage

Responsible: Senior Responder

Support: Incident Owner

Description: Senior Responder should conduct an initial triage of the incident to understand its scope and impact. Available information should be gathered, analysed, and compared to known Tactics, Threats & Procedures (TTP) utilising the MITRE ATT&CK framework and other common knowledge bases. An assessment should then be made of the potential risk to the impacted organisation. Incident Assessment & Triage is to be conducted per the SLA's in Appendix A, based on the initial alert priority where one exists.

NB: The Incident Owner may also assume the role of Senior Responder if **EITHER:** they are already named in the 'Security Incident Response' assignment group **OR** they are experienced / competent to assess security incidents as described in this document.

D5. Assign Sub-Category

Responsible: Senior Responder

Support: N/A

Description: Senior Responder shall classify the incident based on its nature, such as malware infection, data breach, or denial of service (DoS) attack, to determine the appropriate response strategy. See Appendix B for Sub-Category descriptions.

NB: The Incident Owner may also assume the role of Senior Responder if **EITHER:** they are already named in the 'Security Incident Response' assignment group **OR** they are experienced / competent to assess security incidents as described in this document.

D6. Assign Severity

Responsible: Senior Responder

Support: Incident Owner

Description: Senior Responder shall evaluate the severity of the incident. Automated severity assignments from SIEM tools should be considered alongside temporal factors like impact on critical systems, data sensitivity, and business operations of the impacted organisation. See Appendix C for Incident Severity & Priority Assignment Matrix.

NB: The Incident Owner may also assume the role of Senior Responder if **EITHER:** they are already named in the 'Security Incident Response' assignment group **OR** they are experienced / competent to assess security incidents as described in this document.

D7. Assign Priority

Responsible: Senior Responder

Support: Incident Owner

Description: Senior Responder shall determine the incident's priority based on the severity assessment. High and Medium priority incidents warrant immediate escalation, while Low and Informational incidents can be addressed using standard procedures. See Appendix C for Incident Severity & Priority Assignment Matrix.

- Priority Assigned P2, P3 or P4: Ticket de-escalated to Incident Owner to resolve using BAU Process(es) as advised by Senior Responder at D8.
- Priority Assigned P1: Senior Responder to mobilise CSIRT at D9.

NB: The Incident Owner may also assume the role of Senior Responder if **EITHER:** they are already named in the 'Security Incident Response' assignment group **OR** they are experienced / competent to assess security incidents as described in this document.

D8. Resolve using BAU Process

Responsible: Incident Owner

Support: Service Desk

Description: Incident Owner shall apply standard operating procedures and best practices to resolve P2, P3 and P4 priority incidents, aiming to restore normal operations efficiently and within SLA (See Appendix C).

- Incident Resolved: Close Ticket at P6.

D9. Mobilise CSIRT

Responsible: Senior Responder

Support: Incident Owner
Service Desk
Senior Technical / Product Specialists

Description: Upon escalation of incident as P1 priority, the Senior Responder shall assemble a Critical Security Incident Response Team, which may include the Service Desk, other incident responders, forensic analysts, and other relevant experts.

NB: The Incident Owner may also assume the role of Senior Responder from this step onwards if **ONLY:** they are already named in the 'Security Incident Response' assignment group. If not, the ticket should now be escalated to a Senior Responder. Up-to-date Senior Responders are identified in the BOLT work instruction 'Security Cases: How to Escalate for Assessment' and BOLT 'Security Incident Response' assignment group.

D10. Collect Incident Data

Responsible: Senior Responder

Support: Incident Owner
Service Desk
Senior Technical / Product Specialists

Description: Under instruction from the Senior Responder, the Service Desk shall collect detailed data and evidence related to the incident, including system logs, network traffic captures, and any artifacts that may aid in the investigation. The Senior Responder should determine if data may need to be retained for legal purposes post-incident and enforce the Collection of Evidence Process to ensure data is collected following the order of volatility and maintaining integrity of the chain of custody.

D11. Determine Scope

Responsible: Senior Responder

Support: Incident Owner
Service Desk

Description: The Senior Responder shall define the scope of the incident by identifying affected systems, users, and data. This shall inform the extent of the incident's impact.

D12. Identify if Incident Impacts Personally Identifiable Information (PII)

Responsible: Senior Responder

Support: Incident Owner
Service Desk
Customer

Description: The Service Desk should collaborate with the Customer to determine if impacted systems / locations contain Personally Identifiable Information (PII). If so, the Service Desk shall initiate a detailed assessment to determine the extent of the PII exposure or compromise and inform the Senior Responder.

- PII is Impacted: Senior Responder will instigate Data Breach Response Process at D13 alongside the Security Incident Response Process at D14.
- PII is Not Impacted: Senior Responder will instigate Security Incident Response Process at D14.

D13. Data Breach Response Process

Responsible: Senior Responder

Support: Incident Owner
Customer

Description: If a data breach involving PII is confirmed, the Senior Responder shall follow the Data Breach Response Plan, which includes notifying affected individuals, regulatory bodies, and legal counsel in collaboration with the Customer.

D14. Security Incident Response Process

Responsible: Senior Responder

Support: Incident Owner
Service Desk

Description: Once the scope has been determined, under the direction of the Senior Responder the CSIRT shall follow the Security Incident Response Plan, to include containment, eradication, and recovery steps as appropriate to the classification of the incident.

D15. Reassess Incident

Responsible: Senior Responder

Support: Incident Owner
Service Desk
Senior Technical / Product Specialists

Description: The CSIRT should periodically reassess the incident's status, impact, and containment effectiveness to adapt the response strategy as needed.

D16. Determine if Notification is Required

Responsible: Senior Responder

Support: Customer

Description: In collaboration with the Customer, the Senior Responder shall determine if external or internal notifications are required based on legal, regulatory, or contractual obligations.

- Notifications Required: Continue procedure at D17.
- Notifications NOT Required: Continue to Containment Phase at C1.

D17. Determine Notification Communications

Responsible: Senior Responder

Support: Customer

Description: In collaboration with the Customer, the Senior Responder shall coordinate with legal counsel and public relations to develop a communication plan for notifying relevant parties, including affected individuals and regulatory bodies.

D18. Notify Relevant Parties

Responsible: Senior Responder

Support: Customer

Description: In collaboration with the Customer, the Senior Responder shall oversee the execution of the communication plan, ensuring that notifications are sent out accurately and timely.

Containment Phase

C1. Communicate to Stakeholders

Responsible: Senior Responder

Support: Service Desk

Description: Senior Responder shall maintain ongoing communication with stakeholders to provide updates on detection & information gathering efforts, the incident's status and next steps for containment. Communication should also include updated on previously unsuccessful containment efforts if restarting containment phase.

C2. Develop Containment Plan

Responsible: Senior Responder

Support: Service Desk
Senior Technical / Product Specialists

Description: Led by the Senior Responder, the CSIRT should develop a comprehensive containment plan that outlines specific steps and targeted timescales to isolate and mitigate the incident based on the classification and scope identified during the detection phase. Where applicable the containment plan should follow previously established playbooks relevant to the incident classification.

C3. Execute Containment Plan

Responsible: Senior Responder

Support: Service Desk
Senior Technical / Product Specialists

Description: The CSIRT shall implement the containment plan, taking actions to prevent further damage and limit the incident's spread. Any deviation from the agreed containment plan must be discussed with appropriate stakeholders and approved by the Senior Responder.

C4. Assess Containment Measures

Responsible: Senior Responder

Support: Service Desk
Senior Technical / Product Specialists

Description: The CSIRT shall assess whether the incident has been successfully contained based on observed behaviour compared to original IoC's and other pr-defined criteria. Containment must be agreed by Senior Responder and the Service Desk before continuing.

- Containment Successful: Continue to eradication phase at E1.
- Containment NOT Successful: Restart containment phase at C1, develop new containment plan based on lessons learned.

C5. Update Ticket in ITSM

Responsible: Senior Responder

Support: Service Desk

Description: Senior Responder and Service Desk must ensure that ALL actions taken during the containment phase are accurately documented in the ITSM (ITSM). This documentation includes details of containment measures, timestamps, and any identified vulnerabilities, weaknesses and behaviours.

Eradication Phase

E1. Communicate to Stakeholders

Responsible: Senior Responder

Support: Service Desk

Description: Senior Responder shall maintain ongoing communication with stakeholders to provide updates on containment efforts, the incident's status, and next steps for eradication. Communication should also include updates on previously unsuccessful eradication efforts if restarting eradication phase.

E2. Develop Eradication Plan

Responsible: Senior Responder

Support: Service Desk
Senior Technical / Product Specialists

Description: The CSIRT shall create a detailed eradication plan that outlines the specific steps and targeted timescales to completely remove the incident from affected systems and networks. Where applicable the eradication plan should follow previously established playbooks relevant to the incident classification.

E3. Execute Eradication Plan

Responsible: Senior Responder

Support: Service Desk
Senior Technical / Product Specialists

Description: The CSIRT shall implement the eradication plan, taking actions to remove all traces of the incident from affected systems. Any deviation from the agreed eradication plan must be discussed with appropriate stakeholders and approved by the Senior Responder.

E4. Assess Eradication Measures

Responsible: Senior Responder

Support: Service Desk
Senior Technical / Product Specialists

Description: The CSIRT shall assess whether the incident has been successfully eradicated based on observed behaviour compared to original IoC's and other pre-defined criteria. Eradication must be agreed by Senior Responder and the Service Desk before continuing.

- Eradication Successful: Continue to recovery phase at R1.
- Eradication NOT Successful: Restart eradication phase at E1, develop new eradication plan based on lessons learned.

E5. Update Ticket in ITSM

Responsible: Senior Responder

Support: Service Desk

Description: The Senior Responder and Service Desk must ensure that ALL actions taken during the eradication phase are accurately documented in the ITSM. This documentation includes details of eradication efforts, timestamps, and any lessons learned.

Recovery Phase

R1. Communicate to Stakeholders

Responsible: Senior Responder

Support: Service Desk

Description: Senior Responder shall maintain ongoing communication with stakeholders to provide updates on eradication efforts, the incident's status, and next steps for restoring affected systems, services and data. Communication should also include updated on previously unsuccessful recovery efforts if restarting recovery phase.

R2. Develop Recovery Plan

Responsible: Senior Responder

Support: Service Desk
Senior Technical / Product Specialists

Description: The CSIRT shall create a detailed recovery plan that outlines the specific steps and targeted timescales to restore affected systems to normal operation. Where applicable the recovery plan should follow previously established playbooks relevant to the incident classification.

R3. Execute Recovery Plan

Responsible: Senior Responder

Support: Service Desk
Senior Technical / Product Specialists

Description: The CSIRT shall implement the recovery plan, taking actions to restore critical systems and services whilst ensuring their further security. Any deviation from the agreed recovery plan must be discussed with appropriate stakeholders and approved by the Head of Information Security.

R4. Assess Recovery Measures

Responsible: Senior Responder

Support: Service Desk
Senior Technical / Product Specialists

Customer

Description: The CSIRT in collaboration with the Customer shall assess whether systems and services have been successfully recovered. Recovery must be agreed by Senior Responder, Service Desk and Customer before continuing.

- Recovery Successful: Continue to R6 and post-incident phase at P1.
- Recovery NOT Successful: Restart recovery phase at R1, develop new recovery plan based on lessons learned.

R5. Update Ticket in ITSM

Responsible: Senior Responder

Support: Service Desk

Description: The Senior Responder and Service Desk must ensure that ALL actions taken during the recovery phase are accurately documented in the ITSM. This documentation includes details of recovery efforts, timestamps, and any lessons learned.

R6. Communicate to Stakeholders

Responsible: Senior Responder

Support: Service Desk

Description: Senior Responder shall communicate with stakeholders to the incident's status, and next steps for post-incident review and closure of the incident.

Post-Incident Review and Closure

P1. Conduct RCA (Root Cause Analysis)

Responsible: Senior Responder

Support: Service Desk
Senior Technical / Product Specialists

Description: The CSIRT shall conduct a thorough Root Cause Analysis (RCA) to determine the underlying causes of the incident, including vulnerabilities, misconfigurations, or human errors.

P2. Document Findings

Responsible: Senior Responder

Support: Service Desk
Senior Technical / Product Specialists

Description: The Senior Responder must document the findings of the RCA, including the identified root causes, contributing factors, and recommended corrective actions.

P3. Assign Action Owners

Responsible: Senior Responder

Support: Service Desk
Senior Technical / Product Specialists
Customer

Description: The Senior Responder assigns responsibility for implementing the recommended corrective actions and improvements identified during the RCA. Recommended corrective actions shall be communicated to all stakeholders and agreed with the Customer before proceeding to P4.

P4. Update Controls & Policies

Responsible: Senior Responder

Support: Service Desk
Senior Technical / Product Specialists
Customer

Description: The Senior Responder oversees the update of security controls, policies, and procedures based on the lessons learned from the incident and the RCA findings.

P5. Demobilise CSIRT

Responsible: Senior Responder

Support: N/A

Description: The Senior Responder ensures the orderly demobilisation of the CSIRT, releasing team members from their incident response roles.

P6. Close Ticket

Responsible: Senior Responder

Description: Senior Responder shall formally close the incident record in the ITSM, indicating that the incident response process is complete.

X. End Process

Responsible: Senior Responder

Description: The Senior Responder concludes the incident response process.

Deviation

Dependent upon the classification, severity, and scope of the incident it may be appropriate to deviate from the above plan, for instance combining containment, eradication and/or recovery steps into a single plan. This may happen where urgency of action dictates or where planned steps act to achieve multiple results.

If deviation from this plan is appropriate, it must first be agreed by the CSIRT and approved by the Senior Responder. Any deviation from the plan must be documented fully within the ticket.

Maintenance & Testing

It is the responsibility of the Head of Information Security to maintain and update this procedure. The procedure and its components shall be tested no less than annually to ensure its effectiveness.

APPENDIX A: Incident Sub-Categories

Sub-Category	Description
ACCOUNT TAKEOVER	A malicious actor gaining access to a legitimate user's account credentials. Subcategories could include customer, corporate, employee account takeover, etc.
CRIMINAL ACTIVITY	Illegal conduct by an individual, organisation, or other group of malicious actors. Subcategories could include fraud, sabotage, vandalism, etc
DATA BREACH	Data accessed, modified, and/or exfiltrated by an unauthorised entity. Subcategories could include breaches of customer data, privacy data (e.g., PII or PHI), the organisation's proprietary data, etc.
DENIAL-OF-SERVICE	Malicious activity preventing authorised access to resources.
HUMAN ERROR	An accidental, improper, or otherwise ill-chosen act by an individual (e.g., employee, third-party, etc.) which results in processing delays, equipment damage, or compromised data.
LOST / STOLEN ASSET	Lost or stolen systems, equipment, and/or applications (e.g., desktops, laptops, mobile devices, removable media, etc.).
MALICIOUS CODE	Unauthorised software applications designed to access a system, including a variety of forms of hostile, intrusive, or annoying code. Subcategories could include botnets, keyloggers, ransomware, rootkits, trojans, viruses, worms, etc.
POLICY VIOLATION	Failure to comply with applicable laws, regulations, policies, etc. which could result in negative legal or compliance action
SOCIAL ENGINEERING	An attack that exploits human nature and behaviour to convince the target to perform an unauthorised operation or reveal proprietary information. Subcategories could include impersonation, phishing, smishing, vishing, etc.
SYSTEM FAILURE	The failure of or vulnerability in a system which can cause delays in processing, monetary loss, or loss of data. Subcategories could include application failure, network failure, power failure, etc.
THIRD PARTY	An incident originating from or through a third party, causing direct or indirect damage to the organisation. Subcategories could include third-party data breaches, service unavailability, etc
UNAUTHORISED USE	The unapproved use of systems or data.

APPENDIX B: Incident Severity & Priority Assignment

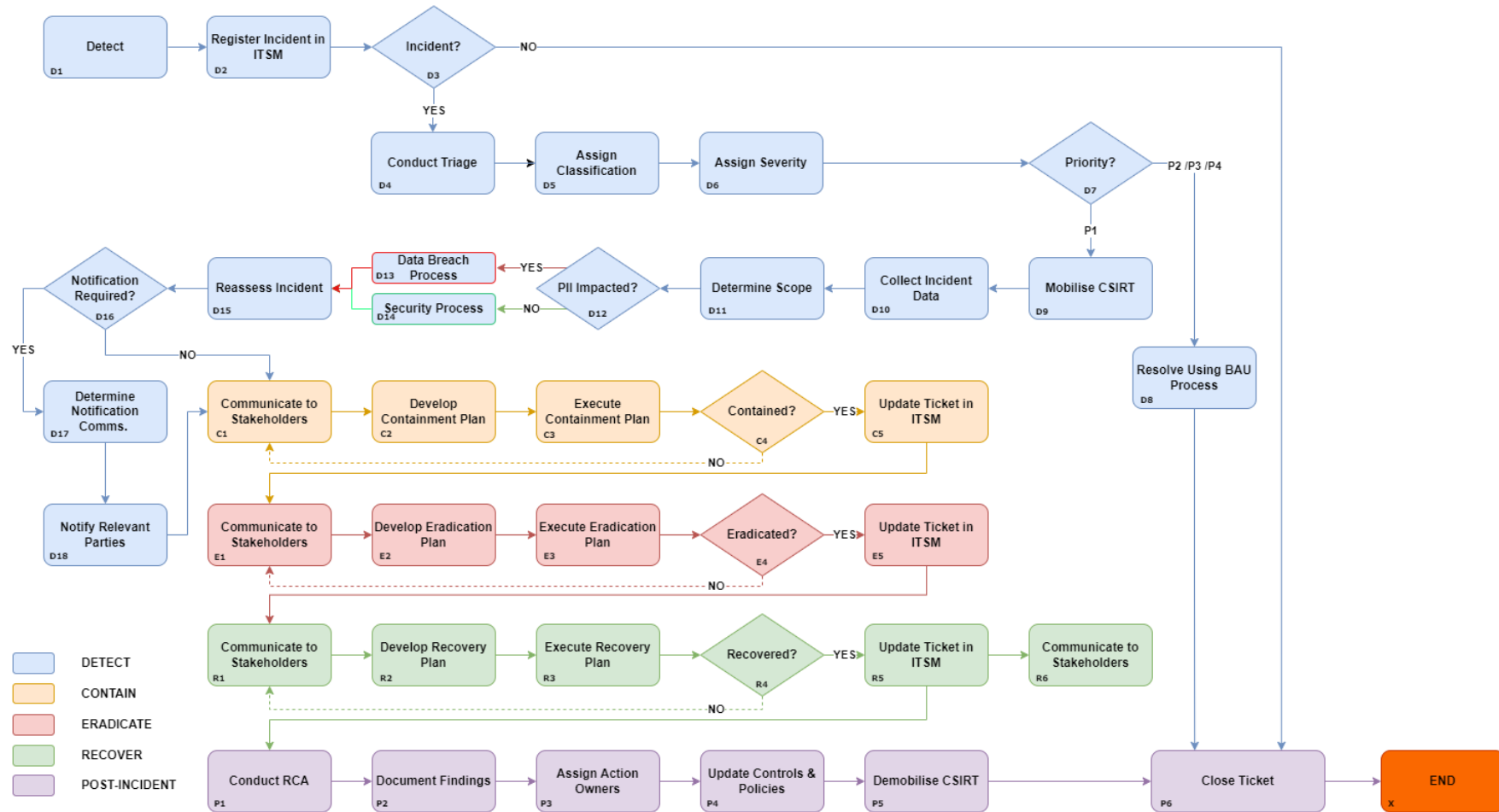
	Occurrence Patterns	Performance Impact	Data Breach	Possible Reputation Impact	Recovery Timeframes & Resources	Projected Financial Costs	Assigned SLA Priority
Insignificant	Historical Not Spreading	None	None	Negligible	Regular	Negligible	P4
Low	Current Not Spreading	Reduced Non-Critical Functions	None	Minimal	Regular	Minimal	P3
Medium	Current Slow Spread	Stopped Non-Critical Functions	Unclassified Data	Moderate	Supplemented	Moderate	P2
High	Current Moderate Spread	Reduced Critical Functions	Proprietary Data	Significant	Extended	Significant	P1
Extreme	Current Fast Spread	Stopped Critical Functions	Proprietary Data	Severe	Irreversible Effects	Severe	P1

APPENDIX C: Incident Priority SLA

SLA Name	Schedule	Hrs	Service SLA relates to
P1 - Response	See BOLT for relevant SLAs		
P1 – Resolution	See BOLT for relevant SLAs		
P2 – Response	See BOLT for relevant SLAs		
P2 – Resolution	See BOLT for relevant SLAs		
P3 – Response	See BOLT for relevant SLAs		
P3 – Resolution	See BOLT for relevant SLAs		
P4 – Response	See BOLT for relevant SLAs		
P4 – Resolution	See BOLT for relevant SLAs		

APPENDIX D: Incident Response Process Map

Incident Response Process Map



APPENDIX E: Responsibility Matrix

Detection Phase		Service Desk	Incident Owner	Senior Responder	Senior Specialists	Customer
D1	Possible Security Incident Detected	●				
D2	Register Incident Ticket in BOLT	●				
D3	Incident Assessment		●	●		
D4	Conduct Triage		●	●		
D5	Assign Sub-Category			●		
D6	Assign Severity		●	●		
D7	Assign Priority		●	●		
D8	Resolve using BAU	●	●			
D9	Mobilise CSIRT	●		●	●	
D10	Collect Incident Data	●		●	●	
D11	Determine Scope	●		●		
D12	Identify if Incident Impacts PII	●		●		●
D13	Data Breach Response Process	●		●		
D14	Security Incident Response Process	●		●		
D15	Reassess Incident	●		●	●	
D16	Determine if Notification is Required			●		●
D17	Determine Notification Communications			●		●
D18	Notify Relevant Parties			●		●
Containment Phase						
C1	Communicate to Stakeholders	●		●		
C2	Development Containment Plan	●		●	●	
C3	Execute Containment Plan	●		●	●	
C4	Assess Containment Measures	●		●	●	
C5	Update Ticket in BOLT	●		●		
Eradication Phase						
E1	Communicate to Stakeholders	●		●		
E2	Develop Eradication Plan	●		●	●	
E3	Execute Eradication Plan	●		●	●	
E4	Assess Eradication Measures	●		●	●	
E5	Update Ticket in BOLT	●		●		
Recovery Phase						
R1	Communicate to Stakeholders	●		●		
R2	Develop Recovery Plan	●		●	●	
R3	Execute Recovery Plan	●		●	●	
R4	Assess Recovery Measures	●		●	●	●
R5	Update Ticket in BOLT	●		●		
R6	Communicate to Stakeholders	●		●		
Post-Incident Phase						
P1	Conduct RCA	●		●	●	
P2	Document Findings	●		●	●	
P3	Assign Action Owners	●		●	●	●
P4	Update Controls & Policies	●		●	●	●
P5	Demobilise CSIRT			●		
P6	Close Ticket			●		
End						
X	End Process			●		

- = Responsible Action Owner
- = Mandatory Support
- = Optional Support