

ARO Critical Operational Incident Response Procedure - Internal

(ISO 27001:2022 Organisational Controls, Clause 5.24)

Author	Greg Nott
Version	1.0
Date Created	01/12/2025
Last Update Date	01/12/2025
Document Control	Released
Document ID	251201-IMS-PRO-AROCriticalOperationalResponseInternal-V1
Security Classification	Confidential

Table of Contents

Approval.....	4
Review.....	4
Change History.....	4
Associated Documents.....	4
Scope.....	5
Purpose.....	5
Procedure.....	5
Detection Phase.....	6
D1. Possible Internal P1 Incident Detected.....	6
D2. Incident Assessment.....	6
D3. Propose Internal P1 Incident	6
D4. Confirm Internal P1 Incident	7
D5. Mobilise P1 Internal Incident Manager	7
D6. Mobilise Internal P1 Incident Team	7
D7. Complete First Management Bridge.....	8
D8. Notify Senior Stakeholders	9
D9. Send Internal P1 Incident Notification.....	9
Resolution Phase.....	10
R1. Develop Investigation and Resolution Plan.....	10
R2. Execute Investigation and Resolution Plan	10
R3. Update Ticket in ITSM	11
R4. Complete Management Bridge Status Update	11
R5. Send Internal P1 Incident Update	12
R6. Continuation Until Resolution.....	12
Resolved Monitoring Phase	12
M1. Incident Resolved or Workaround in Place.....	12
M2. Update Ticket in ITSM.....	13
M3. Send Internal P1 Incident Resolved Status Notification	13
Post-Incident Phase.....	13
P1. Conduct RCA (Root Cause Analysis) and Lessons Learnt Incident Review	13
P2. Document Findings and Actions	14
P3: Distribute Post Internal P1 Incident Report (PMIR)	14
P4. Workaround Removal	14
P5. Assign Action Owners	15

P6. Update Operational Policies & Procedures	15
P7. Demobilise Internal P1 Incident Team	15
P8. Close Ticket	15
X. End Process	15
Deviation	16
Maintenance & Testing	16
APPENDIX A: Incident Classifications	17
APPENDIX B: Incident Severity & Priority Assignment.....	18
APPENDIX D: Incident Response Process Map.....	19
APPENDIX E: Responsibility Matrix	20

Approval

Author	Issue	Approved By	Date
Greg Nott	1.0	Julian Laister	3-Dec-25

Review

Reviewer	Review Criteria	Issue	Date
Julian Laister	ISO 27001:2022	1.0	3-Dec-25

Change History

Author	Change	Issue	Date
Greg Nott	Creation	1.0	01-Dec-25

Associated Documents

Document	Version
Critical Security Incident Response Procedure - Internal	4.0
Critical Incident Business Continuity Response Overlay	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 Operational Incident Response Procedure - Internal 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 operational incident related to internal assets.

Procedure

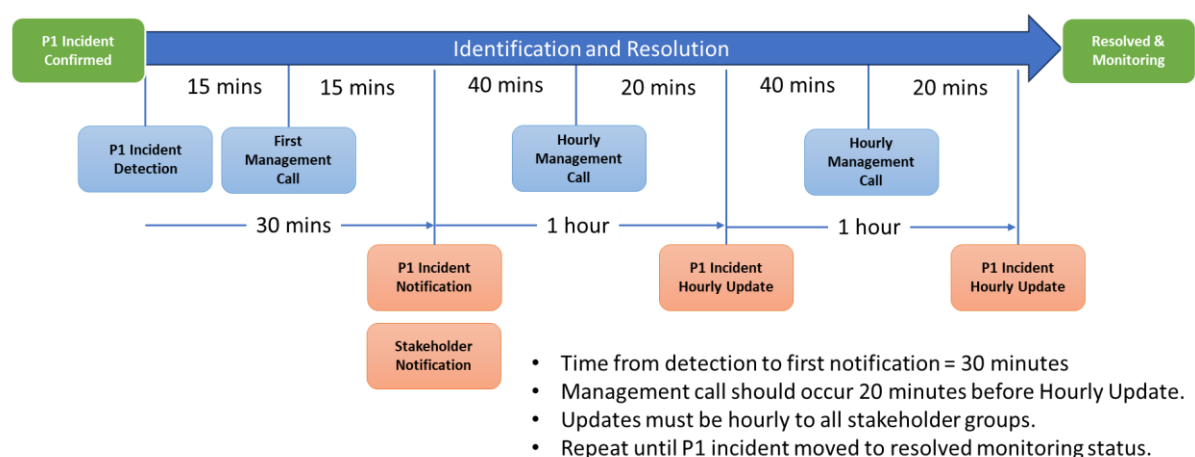
A simplified map of this process is available at Appendix D with responsibilities described throughout the process summarised at Appendix E.

The procedure consists of the following phases:

1. Detection
2. Resolution
3. Resolved and Monitoring
4. Review and Closure

The management and communication cycle through the Identification and Resolution phases is summarised as:

P1 Incident Management and Communication Timeline



Detection Phase

Business Continuity Note: If impact meets Extreme criteria, invoke BCP immediately. (See APPENDIX B: Incident Severity & Priority Assignment).

D1. Possible Internal P1 Incident Detected

Responsible: Incident Owner

Support: IT Team Lead

Description: A potential P1 incident can be identified through a number of channels:

- Proactively during the normal management of cases following standard ITSM processes and procedures.
- Internal inbound notification that they have a high priority issue.
- Employee inbound notification e.g. salesperson, who notifies the IT Team they have an internal business unit with a high priority issue.

This includes the prioritisation of cases based on impact and urgency. A P1 incident can be initially classified based on inputs to urgency and impact by internal business units as well as IT Teams.

D2. Incident Assessment

Responsible: Incident Owner

Support: IT Team Lead

Description: The Incident Owner must assess whether the detected event constitutes a P1 incident based on meeting criteria for urgency and impact per the matrix in Appendix B. If the answer is:

- **Yes** – Internal P1 Incident Proposed: Continue procedure at D3
- **Maybe** - Internal P1 Incident Proposed: Continue procedure at D3
- **No** – Internal P1 Incident Not Confirmed: End procedure at X.

D3. Propose Internal P1 Incident

Responsible: Incident Owner

Support: Group Operations Director
IT Team Lead

Description: Formal confirmation of the P1 incident must be completed by escalating to the Group Operations Director, with liaison with the IT Team Lead.

D4. Confirm Internal P1 Incident

Responsible: Group Operations Director

Support: Incident Owner
IT Team Lead

Description: The Group Operations Director, with any required technical assistance, should quickly triage to confirm the P1 incident, or amend the incident to the correct priority, by correctly classifying urgency and impact. The same criteria as I2 should be used to determine if there is a P1 incident or not.

- **IF SEVERITY ASSIGNED EXTREME:** Invoke Critical Incident Response Continuity Response Overlay.

D5. Mobilise P1 Internal Incident Manager

Responsible: Group Operations Director

Support: Incident Owner
IT Team Lead
Senior Technical Specialists

Description: The Group Operations Director will mobilise the Incident manager. An Internal Incident Manager can only be a trained and approved P1 incident lead, including Technical Team Leads and Information Asset Owners. The Incident Owner should confirm the case number to them, providing a summary, and handing over operational control of the incident to them. The P1 incident manager will:

- Take over operational control for P1 incident.
- Update the case to keep track of actions and decisions made by the management team.

D6. Mobilise Internal P1 Incident Team

Responsible: P1 Internal Incident Manager

Support: IT Team Lead
Incident owner

Description: The P1 incident manager will confirm who will be performing the following roles for the P1 incident:

The Internal P1 Incident Team shall consist of the following roles, in addition to the P1 Internal Incident Manager:

- **Technical Lead** – the senior technical resource who will lead all streams of technical troubleshooting and resolution and coordinate all technical resources working on the P1 incident. The technical lead must ensure that all technical troubleshooting steps are logged in the ITSM system by the technical team, and standard procedures such as change are followed to minimise risk.
- **Communications Lead** – responsible for preparing and sending all internal and external notifications relating to the P1 incident, and ensuring all notifications are sent on-time.

Typically, this would be the P1 Internal Incident Manager, unless the nature of the incident and workload requires a separate person.

- **Field Engineering Lead** - if the service has physical components under the management of Arrow such as CPE, or hosted servers, one or more field engineers should be immediately dispatched to the impacted device or devices, if known. If impacted device is not yet known, field engineers will be put on standby. The field engineer's responsibility will be to act as "eyes and ears", and minimise travel time for smart hands support,
- **Supplier Manager** – required where the incident potentially relates to 3rd party supplier services, for example connectivity or hosted service. The supplier manager's responsibility is to raise and manage the incident with the supplier, act as main interface to the supplier, and ensure the incident is appropriately escalated to minimise outage time. This is probably always going to be the Technical Lead.
- **Other functions** – If at any point in the process, the Internal P1 Incident Team identifies the need for another function or senior stakeholder to participate in the Internal P1 Incident Team to best resolve an issue. The Internal P1 Incident is responsible for confirming a lead from the function, explaining their role and responsibility, and inviting them to the management call.

On confirmation of P1 incident team, the P1 incident manager should confirm team members and standard communication channels to the team.

D7. Complete First Management Bridge

Responsible: P1 Internal Incident Manager

Support: Internal P1 Incident Team

Description: Within no more than 15 minutes from confirmation of P1 incident, the P1 incident manager must start the management bridge. The management bridge must include the following roles as a minimum:

- P1 Internal Incident Manager
- Technical Lead
- Communications Lead
- Supplier Lead
- FE Lead (if applicable)

It is mandatory that all team members attend the bridge to facilitate efficient pooling of knowledge, effective coordination, decision making and accurate communications.

Note: Not attending the call "because I'm fixing the problem" is a false economy and impacts the team's ability to make decisions and communicating effectively with internal business units. At its worst it damages internal business unit satisfaction through poor quality updates, and extending the duration of the fault.

Management call agenda:

- Confirm roles and responsibilities
- Understand the P1 incident background
- Status – Understood current status, and actions to understand P1 incident status

- Impact – Understood impact and actions to understand P1 incident impact
- Internal
- Other internal / external parties
- Identify available engineering resources (FE, L3, Architect), any gaps, and begin dispatching.
- Resolution - If sufficient information is known to determine resolution steps -
Actions to begin resolution.
BC Integration: If resolution steps cannot restore critical internal processes within RTO, escalate to BCP Coordinator and activate alternate processes.
- Agree immediate internal and external comms. Time of 1st Comms send, time required for review/approval, and update frequency.
- Next status call and frequency. The default frequency should be no longer than 1 hour. The status call timing should precede comms updates, so facts can be established once for resolution and communication.

D8. Notify Senior Stakeholders

Responsible: P1 Internal Incident Manager

Support: N/A

Description: The P1 Internal Incident Manager will contact senior and other interested stakeholders to notify them of the P1 incident, confirm ownership and planned communications.

D9. Send Internal P1 Incident Notification

Responsible: Communications Lead

Support: P1 Internal Incident Manager

Description: Notification of P1 incident communication should be sent within the first 30 minutes of confirmation. The Communications Lead will prepare and send the notification of P1 incident. All comms must be proofread and approved by the P1 incident manager prior to sending out. The Communications Lead should check that all related child cases have internal business unit contact information included to ensure internal business units receive updates.

Resolution Phase

Business Continuity Note: If resolution steps cannot restore critical internal processes within RTO, invoke BCP immediately. (See APPENDIX B: Incident Severity & Priority Assignment).

R1. Develop Investigation and Resolution Plan

Responsible: P1 Internal Incident Manager

Support: Incident Owner
Supplier Manager
Senior Technical Specialists

Description: Led by the P1 Internal Incident Manager, the P1 incident team should establish, and continually review a plan that outlines specific steps and targeted timescales to identify, mitigate and resolve the incident.

As a minimum there should always be a “Plan A” and “Plan B”, describing the primary and secondary focus of technical investigation and resolution. A backlog of alternative plans should be managed and reviewed by the P1 incident manager, to ensure that troubleshooting does not halt due to lack of direction.

Multiple approaches are critical as:

- Chosen plans become invalid as they do not solve the issue.
- Time is not wasted as alternative plans can be worked in parallel.
- Long lead time items for alternative plans can be identified and worked on to avoid delay e.g. ordering hardware.

The first stage of the resolution plan is to accurately investigate impact on services and internal business units, identify possible technical areas causing the outage, and take any steps to immediately reduce risk or potential impact to internal business units.

R2. Execute Investigation and Resolution Plan

Responsible: P1 Internal Incident Manager

Support: Incident Owner
Supplier Manager
Senior Technical Specialists

Description: The Incident Owner shall implement the resolution plan, completing the agreed plan steps to investigate and resolve the incident.

R3. Update Ticket in ITSM

Responsible: Internal P1 Incident Team

Support: Incident Owner
Supplier Manager
Senior Technical Specialists

Description: The Internal P1 Incident Team must ensure that ALL actions taken during the containment phase are accurately documented in the ITSM (ITSM).

R4. Complete Management Bridge Status Update

Responsible: P1 Internal Incident Manager

Support: Internal P1 Incident Team

Description: Every hour, at the agreed time, the P1 incident management team must complete the management call to understand status, review and agree containment plan, and communications.

Note: The hourly bridge call must be maintained for a minimum of 3 hours before any different interval should be determined. The management bridge must include the following roles as a minimum:

- P1 Internal Incident Manager
- Incident Owner
- Communications Lead
- Supplier Manager

It is mandatory that all team members attend the bridge.

Agenda of Status Calls:

- Impact – Understood impact – has it changed?
- Technical Update
- Supplier Update
- Service Desk Update (internal business unit)
- Status – Understand status and actions.
- Technical Update
- Supplier Update
- Service Desk Update (monitoring, impacted internal business units, internal business unit escalations)
- Actions since last call
- Containment & Resolution - If sufficient information is known to determine resolution steps - Actions to begin resolution.
- Next actions
- Comms plan – confirm next update and any issues.
- Next status call time.

Status, decisions, and actions should be recorded.

Note: In the event the team feels that they do not have a clear way forwards, or are facing issues they are unable to address, they may choose to escalate to a Senior Stakeholder who can participate on the bridge.

R5. Send Internal P1 Incident Update

Responsible: Communications Lead

Support: P1 Internal Incident Manager

Description: Incident updates must be sent on the agreed next communication times. It is a highly visible indication of our ability to deliver at a critical time, and internal business unit teams may have onward communication commitments based on this. The Communications Lead will prepare and send the notification of P1.

The Communications Lead should check that all related child cases have internal business unit contact information included to ensure internal business units receive updates.

All staff and internal business unit comms must be proofread and approved by the P1 incident manager prior to sending out.

R6. Continuation Until Resolution

Responsible: P1 Internal Incident Manager

Support: Internal P1 Incident Team

Description: The steps identified in the Resolution phase should be continued until a resolution or workaround resolves the issue, and internal business unit services are returned.

Business Continuity Note: If resolution steps cannot restore critical internal processes within RTO, invoke BCP immediately. (See APPENDIX B: Incident Severity & Priority Assignment).

Resolved Monitoring Phase

Business Continuity Stand-down Criteria: Confirm normal operations restored and alternate processes deactivated before closure.

M1. Incident Resolved or Workaround in Place

Responsible: P1 Internal Incident Manager

Support: Internal P1 Incident Team

Description: The P1 incident is resolved once the cause of the P1 incident has been resolved, and all internal business unit services returned. A P1 incident can only be determined to be Resolved on an Internal P1 Incident Management call in agreement with each member of the P1 incident team.

- A P1 incident may be determined to be resolved where a workaround has been put into place. This can be considered acceptable if all services are returned to internal business

units, the risk of repeat failure has been removed, but there is additional work to return services to normal operation.

- The internal business unit must always be consulted to get agreement that services have returned to agreed levels before the incident can be resolved.
- Where there is still high risk of P1 incident, the P1 incident should not be considered resolved, and troubleshooting and resolution activities should continue.
- Once resolution is agreed an update should be sent to internal business units.

M2. Update Ticket in ITSM

Responsible: Internal P1 Incident Team

Support: N/A

Description: The Internal P1 Incident Team must ensure that ALL actions taken during the resolution phase are accurately documented in the ITSM. This documentation includes details of resolution efforts, timestamps, and any lessons learned.

M3. Send Internal P1 Incident Resolved Status Notification

Responsible: Communications Lead

Support: Internal P1 Incident Team

Description: Once resolution is agreed an update should be sent. All comms must be proofread and approved by the P1 incident manager prior to sending out.

Post-Incident Phase

Business Continuity Note: Include BC lessons learned and confirm any BCP invocation effectiveness.

P1. Conduct RCA (Root Cause Analysis) and Lessons Learnt Incident Review

Responsible: P1 Internal Incident Manager

Support: Internal P1 Incident Team

Description: The P1 Internal Incident Manager shall conduct a review within 2 working days of resolution of the incident including:

- **Incident Review** - Thorough Root Cause Analysis (RCA) to determine the underlying causes of the incident, including misconfigurations, or human errors.
- **Internal P1 Incident Process Review** - Lessons Learnt to determine how well the P1 incident process worked, any failures and any improvements to be implemented.

Agenda for the review:

- Incident Review
 - Review of P1 incident timeline and issues
 - Impact – internal business unit services.

- Impact – internal CG services.
- Root cause analysis – things that should have worked.
- Service improvements – improvements to avoid issues again.
- Internal P1 Incident Process Review
 - P1 incident process walkthrough and issues. Did we follow process?
 - Failures and improvements
- Key risks for risk register.
- Action plan and suggested owners

P2. Document Findings and Actions

Responsible: P1 Internal Incident Manager

Support: Internal P1 Incident Team

Description: The P1 Internal Incident Manager must document the findings of the RCA and Lessons Learnt Review including the identified root causes, contributing factors, and recommended corrective actions. Lessons Learnt including what worked well, failures, and recommended improvements.

P3: Distribute Post Internal P1 Incident Report (PMIR)

Responsible: P1 Internal Incident Manager

Support: Internal P1 Incident Team

Description: The P1 Internal Incident Manager shall produce a Post Internal P1 Incident Report and distribute within 5 working days of resolution of the incident including thorough Root Cause Analysis (RCA) to determine the underlying causes of the incident, including misconfigurations, or human errors.

Before distribution the PMIR should be reviewed and approved by the Group Operations Director. The PMIR should be distributed to all internal business units who have requested a PMIR, senior internal stakeholders and related internal owners e.g. account managers and service delivery managers.

P4. Workaround Removal

Responsible: P1 Internal Incident Manager

Support: Internal P1 Incident Team

Description: The P1 Internal Incident Manager should ensure that plans to remove the workaround are in place before the closure of the P1 incident. This would be completed during the Review and Closure phase, by agreeing ownership of the workaround removal plan. Include BC lessons learned and confirm any BCP invocation effectiveness.

P5. Assign Action Owners

Responsible: P1 Internal Incident Manager

Support: Internal P1 Incident Team
Group Operations Director

Description: The P1 Internal Incident Manager assigns responsibility for implementing the recommended corrective actions and improvements identified during the RCA and Lessons Learnt. Recommended corrective actions shall be communicated to all stakeholders and agreed. If necessary, the P1 Internal Incident Manager should setup one or more action reviews, to monitor action progress. Critical actions should be completed within 5 working days.

P6. Update Operational Policies & Procedures

Responsible: Group Operations Director

Support: Internal P1 Incident Team

Description: The Group Operations Director is responsible for the update of ITSM policies and procedures based on the lessons learned from the incident and the RCA findings.

P7. Demobilise Internal P1 Incident Team

Responsible: P1 Internal Incident Manager

Description: The P1 Internal Incident Manager ensures the orderly demobilisation of the Internal P1 Incident Team, releasing team members from their incident response roles.

P8. Close Ticket

Responsible: P1 Internal Incident Manager

Description: The P1 Internal Incident Manager shall formally close the incident record in the ITSM, including all parent and child cases, indicating that the incident response process is complete.

X. End Process

Responsible: P1 Internal Incident Manager

Description: The P1 Internal Incident Manager 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 Internal P1 Incident Team and approved by the Group Operations Director. Any deviation from the plan must be documented fully within the ticket.

Maintenance & Testing

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

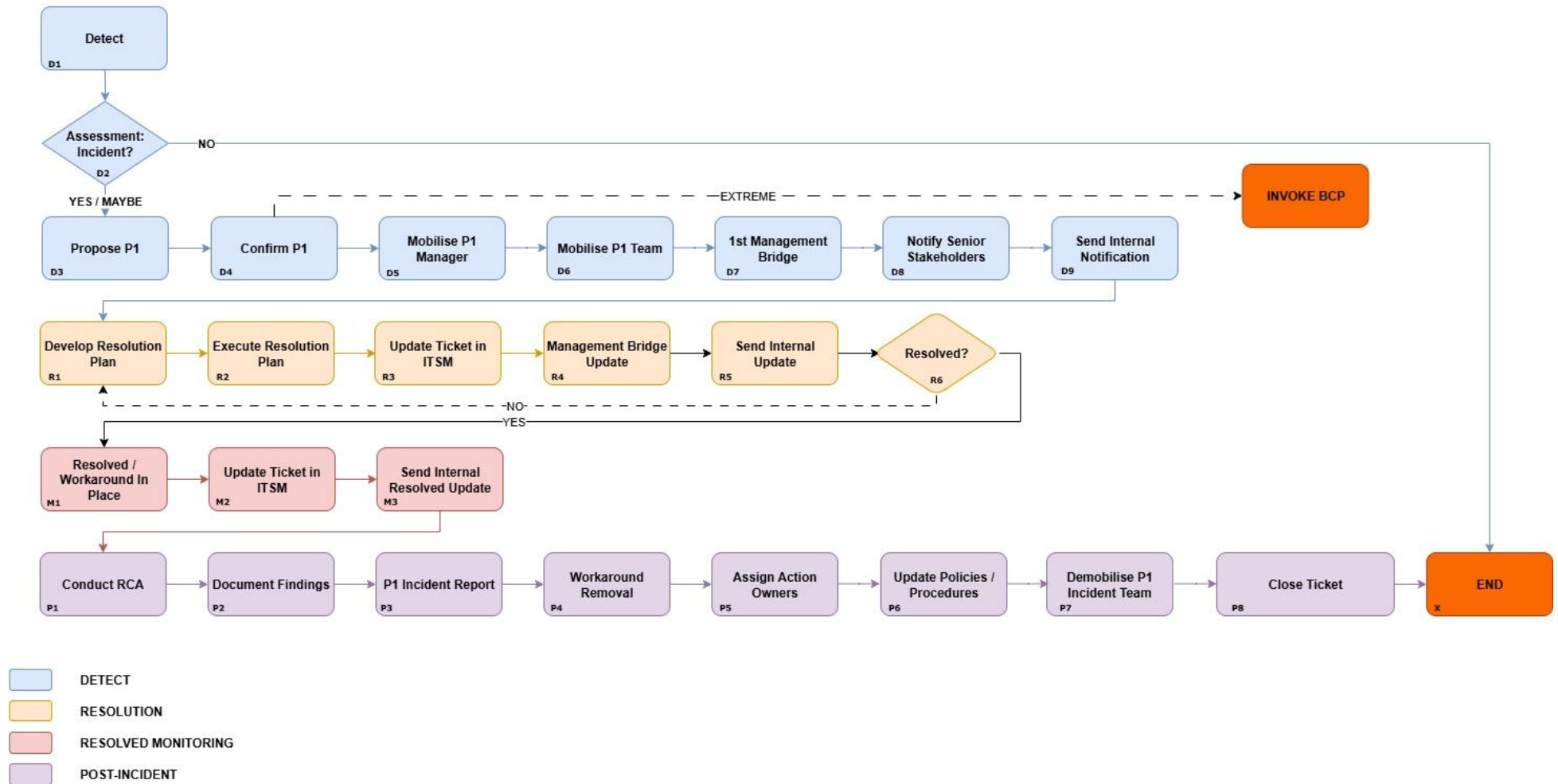
APPENDIX A: Incident Classifications

Classification	Description
SERVICE OUTAGE	Complete loss of a critical internal service (e.g., email, ERP, authentication).
SERVICE DEGRADATION	Significant performance issues impacting business processes.
APPLICATION FAILURE	Failure of a core business application or module.
INFRASTRUCTURE FAILURE	Hardware or virtualization platform failure (servers, storage, network).
NETWORK CONNECTIVITY	Loss or degradation of LAN/WAN connectivity internally or to cloud services.
POWER / FACILITIES	Power outage, cooling failure, or other facilities-related IT disruption.
BACKUP / RESTORE FAILURE	Repeated backup job failures or inability to restore critical data.
CHANGE FAILURE	Failed internal change causing service disruption or instability.
THIRD-PARTY SERVICE ISSUE	Outage or degradation of a vendor-managed service impacting internal operations.
HUMAN ERROR	Accidental misconfiguration or operational mistake causing disruption.
CAPACITY / RESOURCE ISSUE	Resource exhaustion (CPU, memory, storage) impacting critical services.

APPENDIX B: Incident Severity & Priority Assignment

	Occurrence Patterns	Service Impact	Customer Impact	Regulatory / Contractual Impact	Recovery Timeframes & Resources	Projected Financial Costs	Assigned SLA Priority
Insignificant	Historical Not Recurring	None	None	None	Regular	Negligible	P4
Low	Current Isolated	Minor Degradation Non-Critical Service(s)	Minimal Inconvenience	None	Regular	Minimal	P3
Medium	Current Limited Spread	Partial Outage Non-Critical Service(s)	Moderate Inconvenience	Possible Minor Breach of SLA	Supplemented	Moderate	P2
High	Current Widespread	Outage Critical Service(s)	Significant Customer Impact	SLA Breach Likely	Extended	Significant	P1
Extreme	Current Rapid Escalation	Complete Outage Critical Service(s)	Severe Customer Impact	SLA Breach Certain / Regulatory Exposure	Irreversible Effects	Severe	INVOKE BCP

APPENDIX D: Incident Response Process Map



APPENDIX E: Responsibility Matrix

Detection Phase		Incident Owner	IT Team Lead	Group Ops Director	Incident Manager	Comms Lead	Senior Specialists	Supplier Manager(s)	Incident Team
D1	Possible Internal P1 Incident Detected	●	●						
D2	Incident Assessment	●	●						
D3	Propose Internal P1 Incident	●	●	●					
D4	Confirm Internal P1 Incident	●	●	●					
D5	Mobilise P1 Internal Incident Manager	●	●	●			●		
D6	Mobilise Internal P1 Incident Team	●	●		●				
D7	Complete First Management Bridge				●				●
D8	Notify Senior Stakeholders				●				
D9	Send Internal P1 Incident Notification				●	●			
Resolution Phase									
R1	Develop Investigation and Resolution Plan	●			●		●	●	
R2	Execute Investigation and Resolution Plan	●			●		●	●	
R3	Update Ticket in ITSM	●			●		●	●	
R4	Complete Management Bridge Status Update				●				●
R5	Send Internal P1 Incident Update				●	●			
R6	Continuation Until Resolution				●				●
Resolved Monitoring Phase									
M1	Incident Resolved or Workaround in Place				●				●
M2	Update Ticket in ITSM								●
M3	Send Internal P1 Incident Resolved Notification					●			●
Post-Incident Phase									
P1	Conduct RCA (Root Cause Analysis)				●				●
P2	Document Findings and Actions				●				●
P3	Distribute Post Internal P1 Incident Report				●				●
P4	Workaround Removal				●				●
P5	Assign Action Owners			●	●				●
P6	Update Operational Policies & Procedures			●					●
P7	Demobilise Internal P1 Incident Team				●				
P8	Close Ticket				●				
End									
X	End Process				●				
● = Responsible Action Owner ● = Mandatory Support ● = Optional Support									