HAWK INCIDENT AND BC/DR POLICY

Data Classification	**Public**
Author	Ira Goel
Approver	Management
Approved Date	Dec 09, 2024
Effective From	Dec 12, 2024
Current Version	1.0

1.0 Introduction

Hawk's Incident, Business Continuity (BC) and Disaster Recovery (DR) Policy is designed to address the strategic impact to business as caused by incidents and events whether internal or external.

2.0 Purpose

The policy covers three topics:

- Incident management,
- Business continuity, and
- Disaster recovery

The policy provides Hawk's strategic and high-level structure on the approach managing incidents, operational resilience and disaster recovery.

3.0 Scope

The policy applies to:

1. All Hawk-managed offices, and facilities,
2. Business critical cloud production environments, particularly the AML services Hawk provides to its clients, and
3. All employees and involved people-resources.

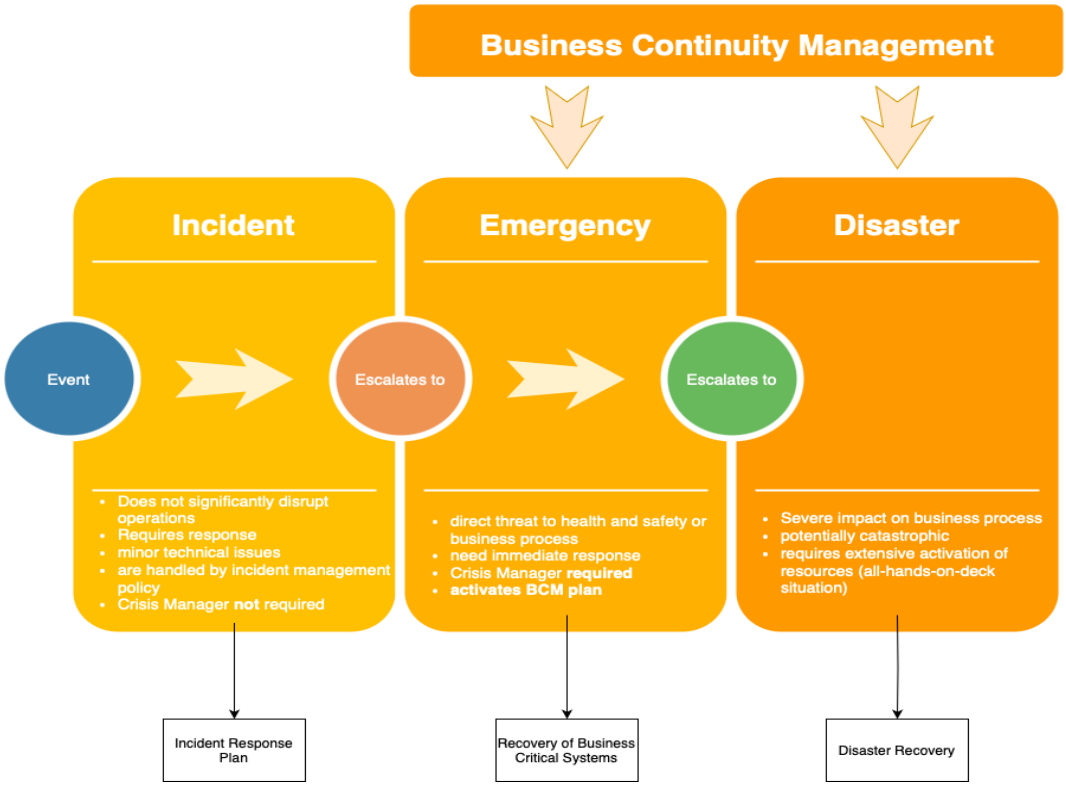
4.0 Definitions

- **Backup**: The process of copying and archiving HAWK's business data and systems to ensure data can be restored in the event of loss or destruction.
- **Business Continuity Management (BCM)**: BCM at HAWK refers to a comprehensive management process that identifies potential threats to the company and the impacts those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response. The aim is to safeguard the interests of its key stakeholders, reputation, brand, and value-creating activities.
- **Business Continuity Plan (BCP)**: This is the documentation of the general framework and set of instructions or procedures that describe how HAWK will respond to an emergency, including the allocation of resources, sequence of actions, and responsibilities. The BCP is designed to ensure the continuation of vital business operations during and after a disaster.
- **Business Continuity Strategy**: This policy outlines the strategy HAWK employs to ensure critical operations continue during and after a disaster.
- **Business Impact Analysis (BIA)**: BIA is the process by which HAWK determines and evaluates the potential effects of an interruption to critical business operations due to a disaster, accident, or emergency.
- **Critical Services**: These functions are essential to HAWK's ability to deliver its core services and products. Without these functions, the company would not be able to maintain its business operations.

- **Disaster**: A disaster is a severe, potentially catastrophic event that causes significant disruption to HAWK's operations or infrastructure. Disasters are characterized by their scale and impact, necessitating extensive recovery efforts and mobilization of resources to rebuild and recover from the damage inflicted.
- **Disaster Recovery (DR)**: This refers to the specific steps HAWK undertakes to resume business operations following a catastrophic event. DR focuses on the IT or technological systems that support business functions.
- **Emergency**: An emergency is a sudden, urgent event that poses a direct threat to health and safety, the environment, or HAWK's critical functions. Emergencies require immediate response actions to prevent further harm.
- **Emergency Handbook**: The Emergency Handbook identifies specific vulnerabilities and recommends business continuity procedures by scenario to prevent extended service outages.
- **Incident**: An incident is an event that may not significantly disrupt operations but requires a response to prevent escalation. Incidents at HAWK can range from minor technical issues to more significant problems that could impact service delivery.
- **Recovery Point Objective (RPO)**: This refers to the maximum tolerable amount of data that might be lost in a specific timeframe due to a major incident before significant damage occurs.
- **Recovery Time Objective (RTO)**: This is the duration within which HAWK's business functions must be restored to ensure business continuity.
- **Resilience**: The ability of HAWK to withstand and recover from incidents and rapidly adapt and respond to changes and opportunities.
- **Risk Assessment**: This is the process HAWK uses to identify and evaluate risks to its operations, considering the likelihood and impact of various threats.
- **Stakeholders**: Stakeholders are individuals or groups that have an interest in HAWK's operations and outcomes. This can include employees, customers, partners, investors, suppliers, and regulatory bodies.

5.0 Incident Response, Business Continuity and Disaster Recovery

The following diagram shows the interconnection between incident response, business continuity and disaster recovery, and Hawk's approach to these practices.



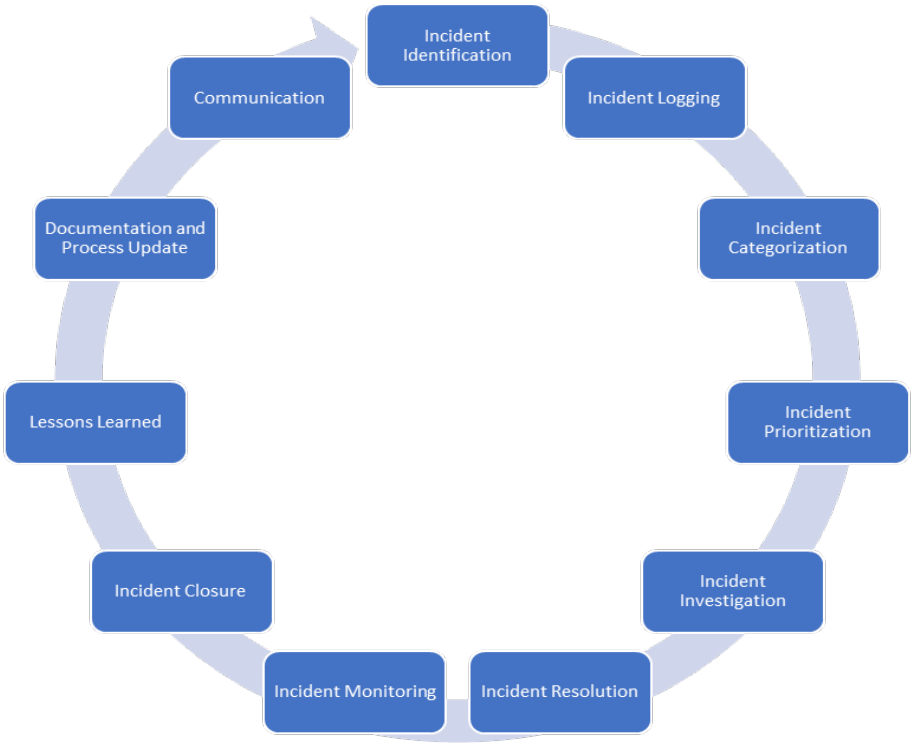
5.1 Incident Response

Hawk has a risk-based approach to manage and respond to incidents. The incident is identified, assessed, classified, categorized and triaged based on impact. Hawk categorizes the incidents as:

- Major Incident or Emergency,
- Data Breach, and
- Functional or Technical Incident.

Hawk measures severity of an incident as Critical, High, Medium and Low.

In general, Hawk's incident response process follows the steps shown in the diagram.



5.2 Business Continuity and Disaster Recovery

Hawk's business continuity plan aims to prepare Hawk in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.

Hawk's business continuity management follows industry best practices and standards such as ISO 27001, SO 2 Type 2 and ISO/IEC 22301. Business continuity plans are triggered for Emergency or Major incidents based on the severity assessment.

Exclusions

The following scenarios are excluded from the BC/DR plan scope:

- A national disaster, such as a nuclear war in the EU, is beyond the scope of this plan

In an event for such scenario, the Management confers with all relevant stakeholders to determine the appropriate response.

Hawk has identified critical business services after performing business impact assessment and the continuity strategy. List of the critical services are:

Critical System/Service	Continuity Strategy
Production Cloud Environment	1. Availability zones for redundancy 2. Cloud service provider SLA commitments for data center availability and recovery

Productivity Software	Cloud based solution with standard SLA with the provider
Accounting and HR	Cloud based solution with standard SLA with the provider
Sales and Marketing	Cloud based solution with standard SLA with the provider

5.3 Communications and Escalations

Incidents and events are escalated to Hawk Management based on the escalation plan. The Management or Team leads are notified of any disaster affecting Hawk facilities or operations. Communication occurs predefined regular channels, including phone calls, email, or other means.

6.0 Hawk's Practices and Team

Hawk's incident response, business continuity and disaster recovery practices are combination of industry standards and best practices; and are attested under ISO 27001 and SOC 2 Type certifications.

Hawk's information security and privacy team, includes an Information Security Officer, Data Protection Manager, and team members. The Information Security Officer is also the Global Incident Manager and the main point of contact in case of an incident.

Hawk's clients should contact their customer success manager at Hawk to report an incident or email security@hawk.ai.

7.0 Policy Governance

Any violations to any Hawk Policy must be reported to the Information Security Officer at security@hawk.ai.

All Hawk personnel (including employees, contractors, and relevant third parties) must maintain the security, confidentiality, availability, integrity, and privacy of Hawk assets. Violations of Hawk policies and procedures may be considered severe breaches of trust, resulting in disciplinary action up to and including termination of employment or contract and prosecution following applicable federal, state, and local laws.