

**Task.** Respond to a Category 1 Incident.

**Purpose.** The organization must be able to respond to the risk introduced by Category 1 incidents, otherwise known as “root-level intrusions,” to protect the usability and defensibility of its enterprise.

**Conditions.**

- **Incident Response Team.** The organization is staffed with personnel who possess the knowledge, skills, attributes, processes, and technology required to perform in the following DoD Cybersecurity Workforce Framework (DCWF) Work Roles: Information Systems Security Manager (ISSM), Incident Responder, Infrastructure Support Specialist, System Administrator, and Network Administrator.
- **Stakeholders.** The organization is able to call and email the following stakeholders: Information Owner, Information System Owner, commander, and Tier III (Installation) Cyber Security Service Provider (CSSP).
- **Incident Criteria.** The organization suspects the following activity has occurred: an Information System (IS) was accessed by a privileged account (e.g., domain administrator, local administrator, etc.) without authorization and/or malicious logic that provides remote, interactive control was installed/executed.

**Standard.** The organization was able to contain the incident, determine the root cause, eradicate the threat/vulnerability, restore operations, implement lessons learned, and communicate with its stakeholders throughout each phase.

## Analysis Phase

Bridge the gap between what was perceived and what actually happened. Using the Data Sources suggested, search for answers to the Questions listed below. If enough evidence suggests a Category 1 incident occurred, create a report with the information available and execute Containment procedures immediately (see next page). Otherwise, re-categorize the event as Category 8 “Investigating” or Category 9 “Explained Anomaly.” At the end of every incident response phase, update your report with any new Reportable Details collected and/or generated.

### Data Sources

- Network: IDS alerts, NetFlow records, transactions (i.e., HTTP, DNS, SMB queries), statistics, and PCAP files.
- Host: memory artifacts (i.e., network connections, processes, services, scheduled tasks, etc.) and disk artifacts (logs, accounts, files, Windows Registry keys, etc.).

### Questions

- What account was used to access the IS in question?
- Does this account have elevated privileges?
- During what time periods did someone access and/or attempt to access IS in question?
- What in memory and/or on disk was accessed, modified, added, or removed on the IS in question?
- Who had access (i.e., knew the password, PIN, etc.) to the account in question?
- Were they working during the time periods of interest?
- Did they have authorization to (1) access the account and (2) conduct the activity observed (3) on the IS in question (4) during the time periods of interest?
- What other ISs did this person, account, and/or IS in question access and/or attempt to access?

### How to Investigate

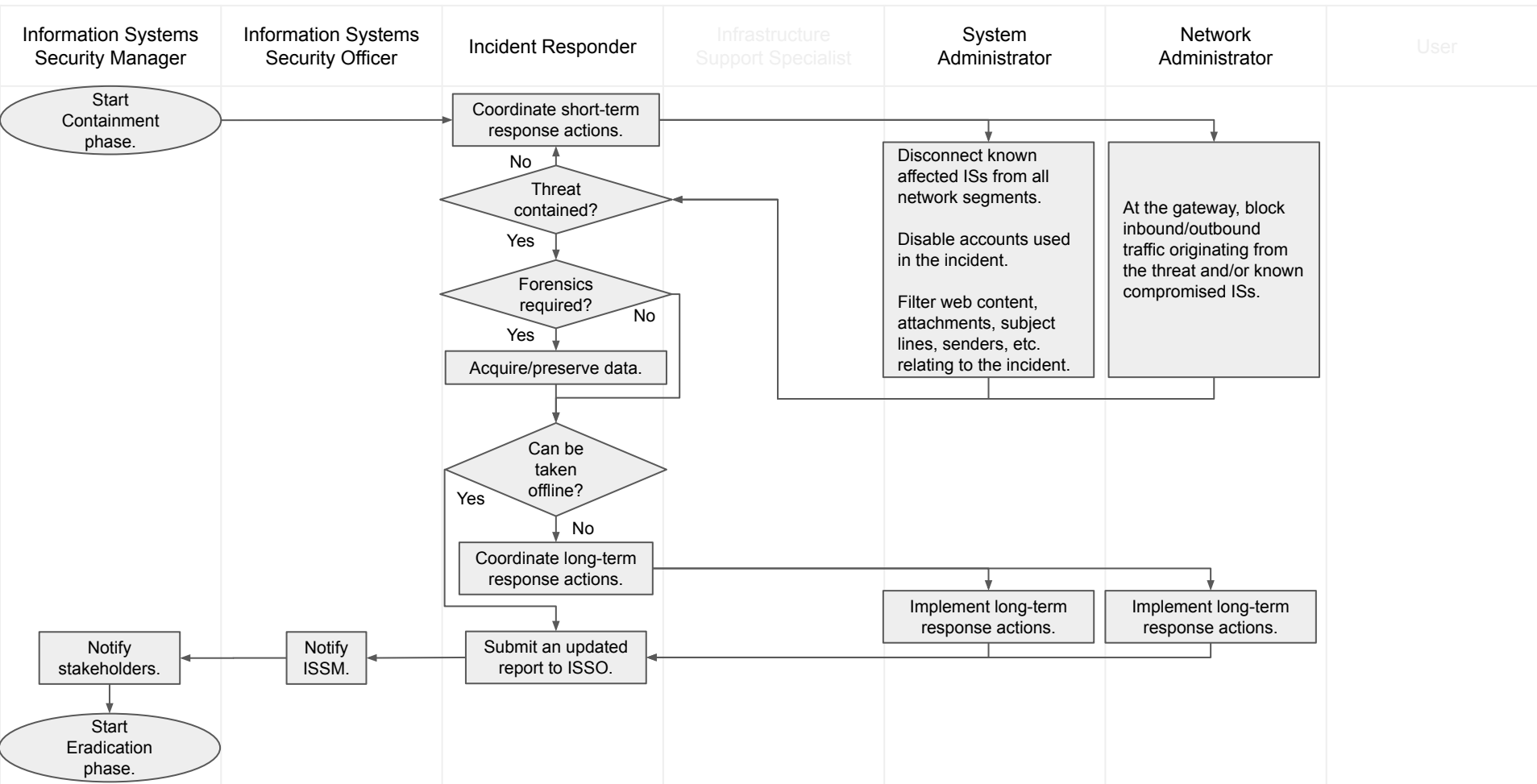
- Select one of the Data Sources above, pick a field within it, and search other data sources for the value it contains. Repeat until you collect enough findings to suggest an incident has occurred.

### Reportable Details

- Date-Time Groups (DTG) of when the incident started and was detected, contained, and resolved.
- Primary Point-of-Contact (POC) and alternate POC for incident.
- Category, summary, and root-cause of incident.
- Hostname, IP address, MAC address, make/model, serial number of devices affected.
- All actions taken (include the 5 Ws).

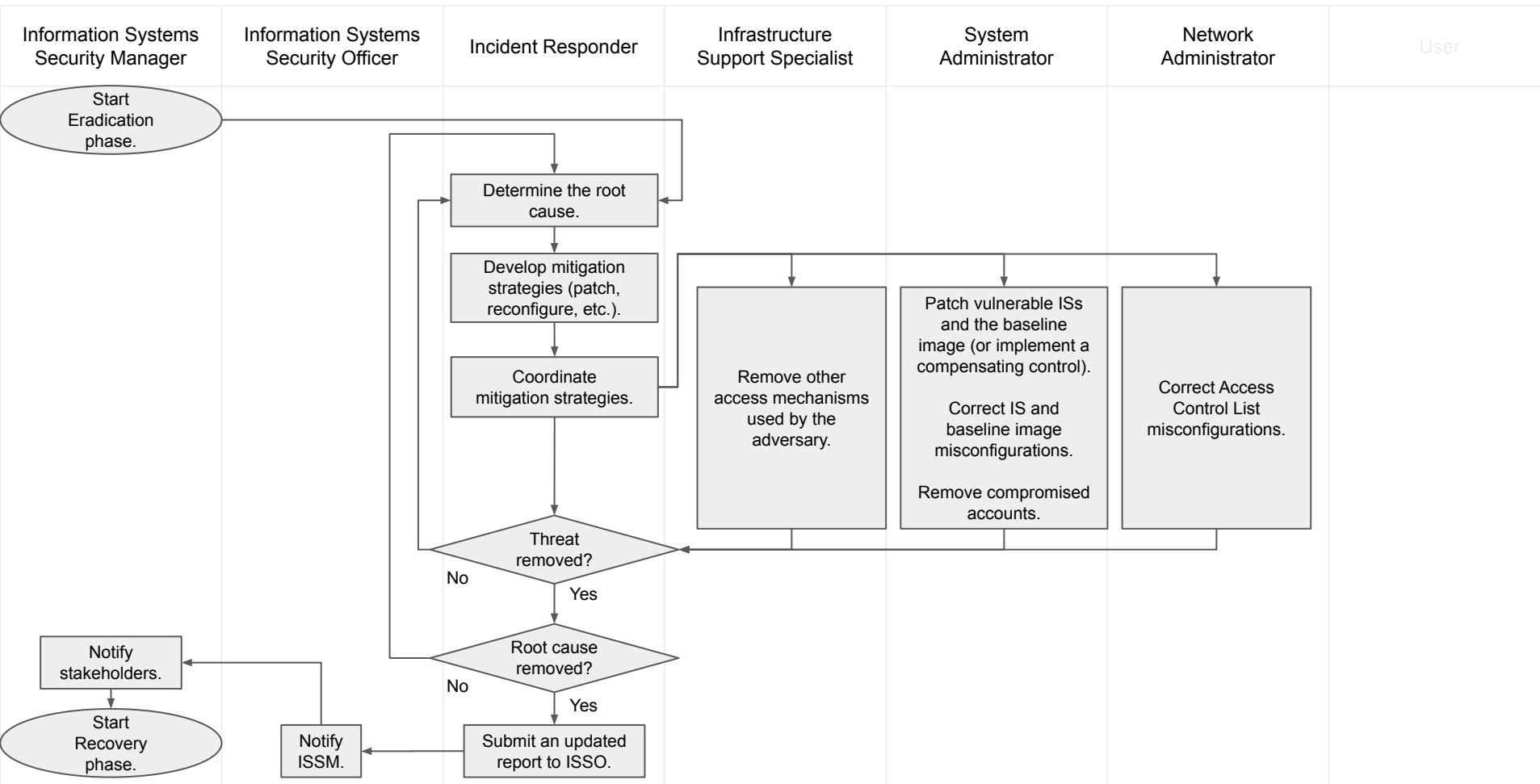
# Category 1 Incident Response Plan

## Containment Phase



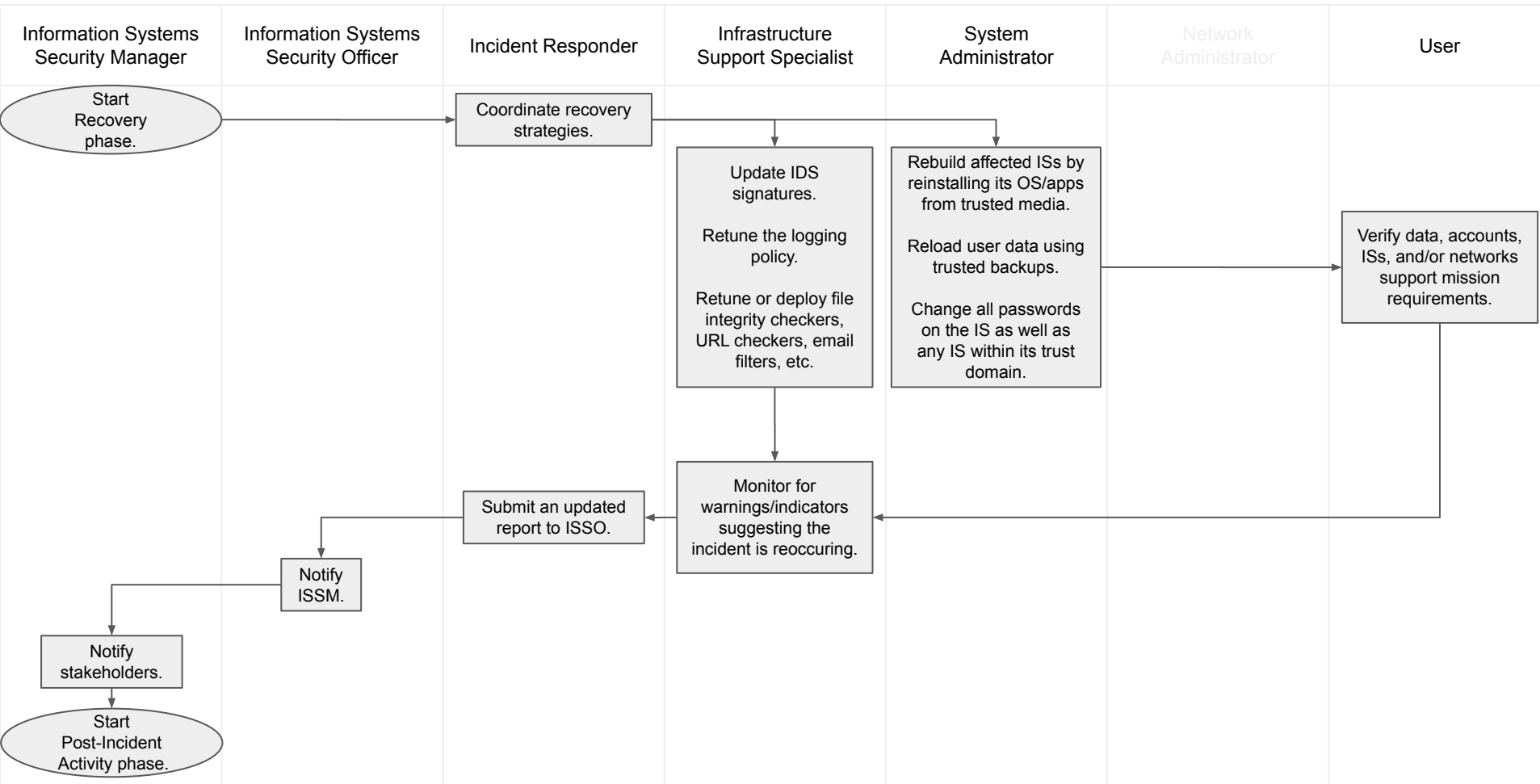
# Category 1 Incident Response Plan

## Eradication Phase



## Category 1 Incident Response Plan

### Recovery Phase



## Category 1 Incident Response Plan

### Post-Incident Activity Phase

