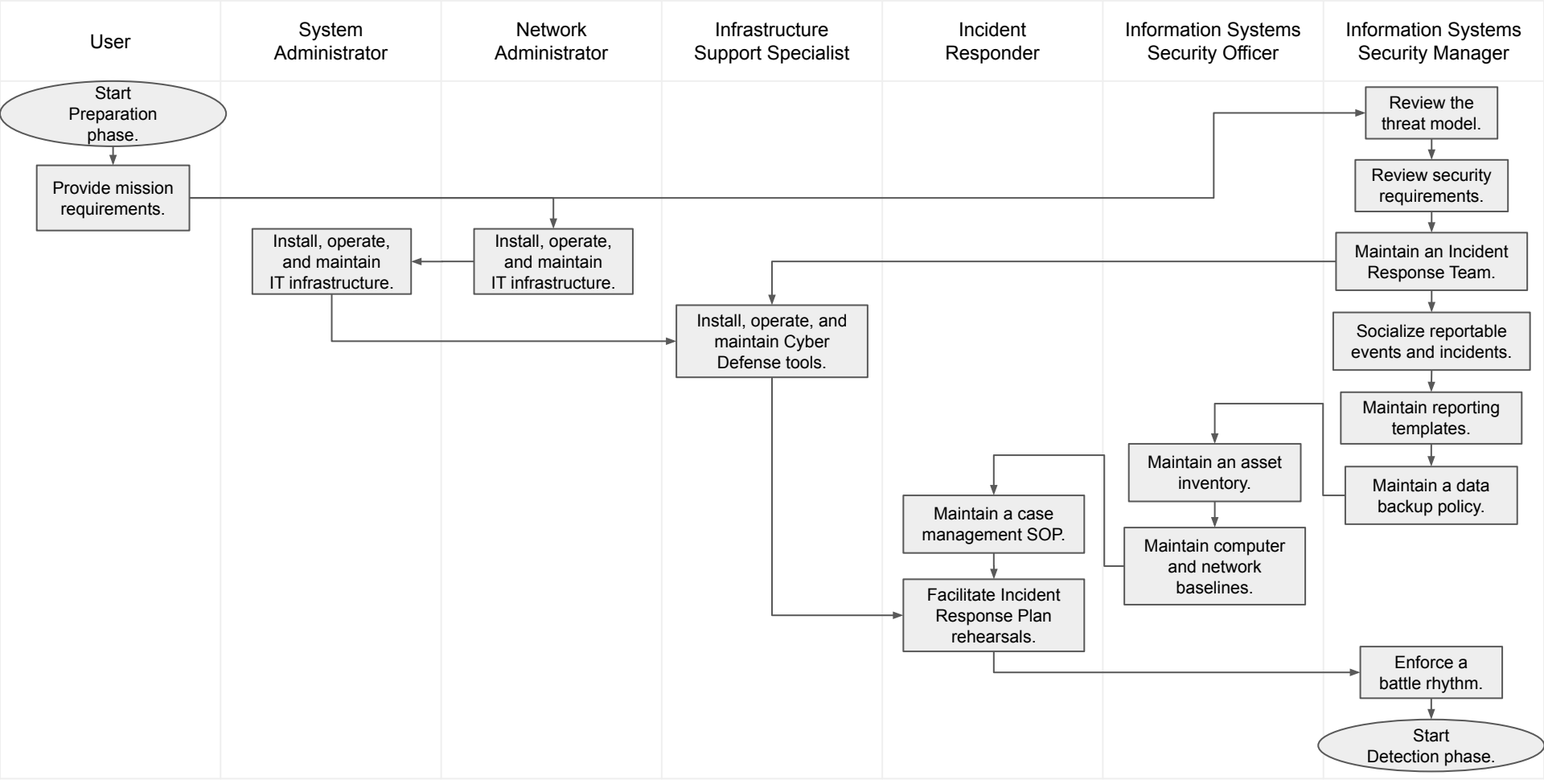
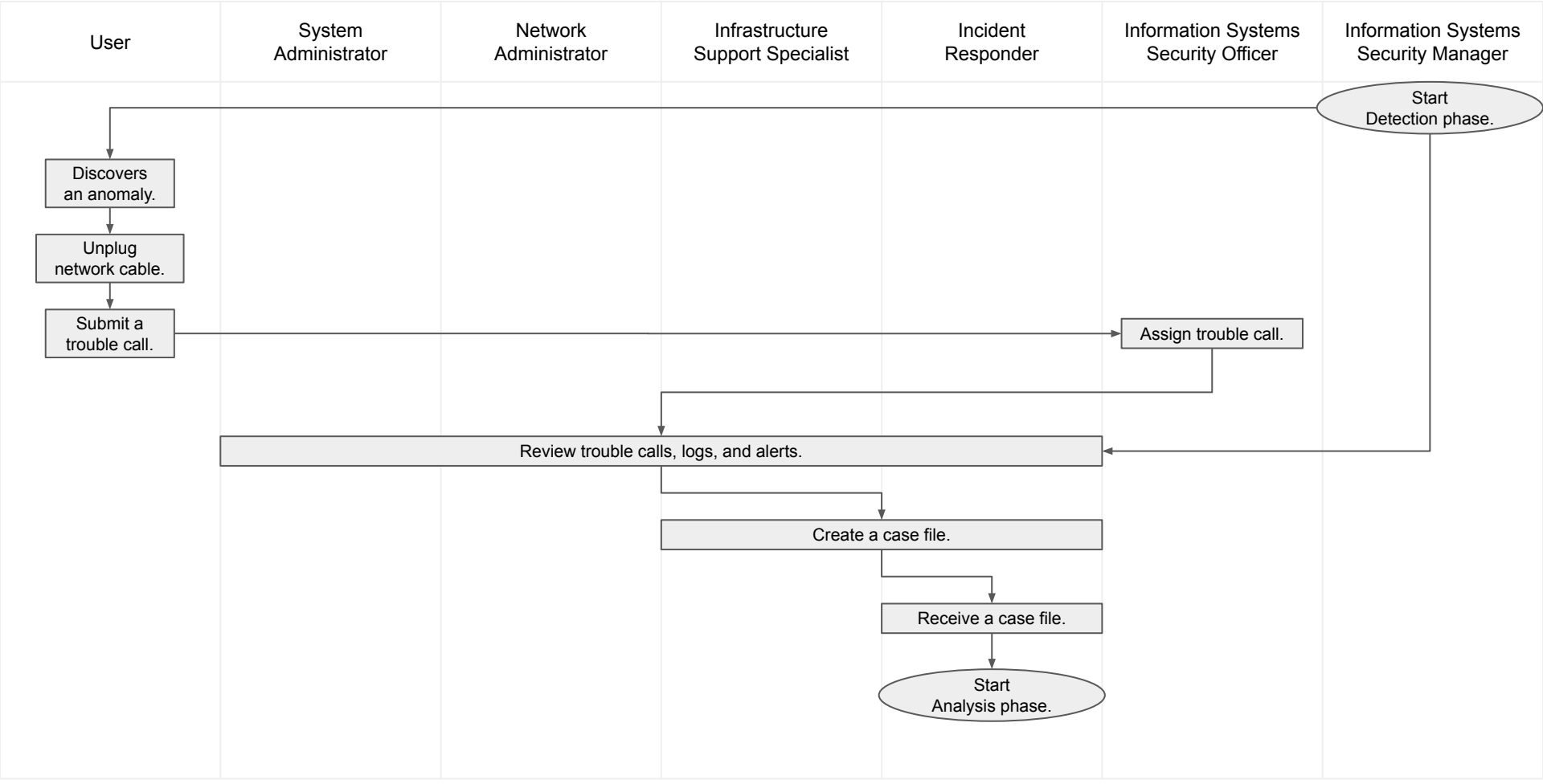
Incident Handling
Preparation Phase

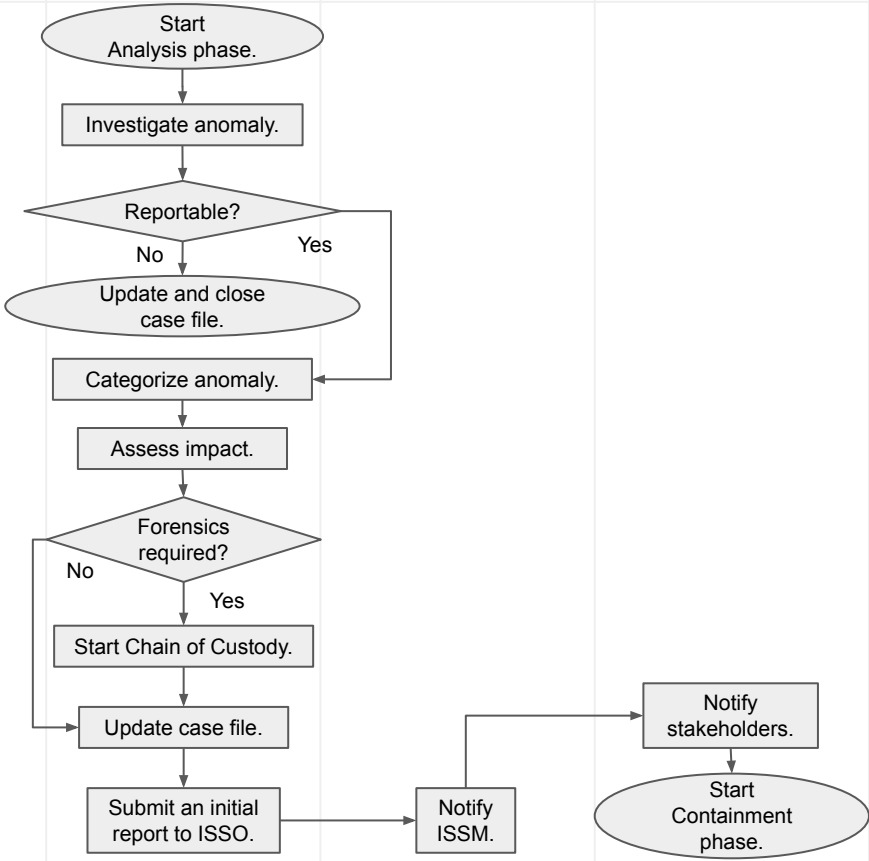


Incident Handling
Detection Phase

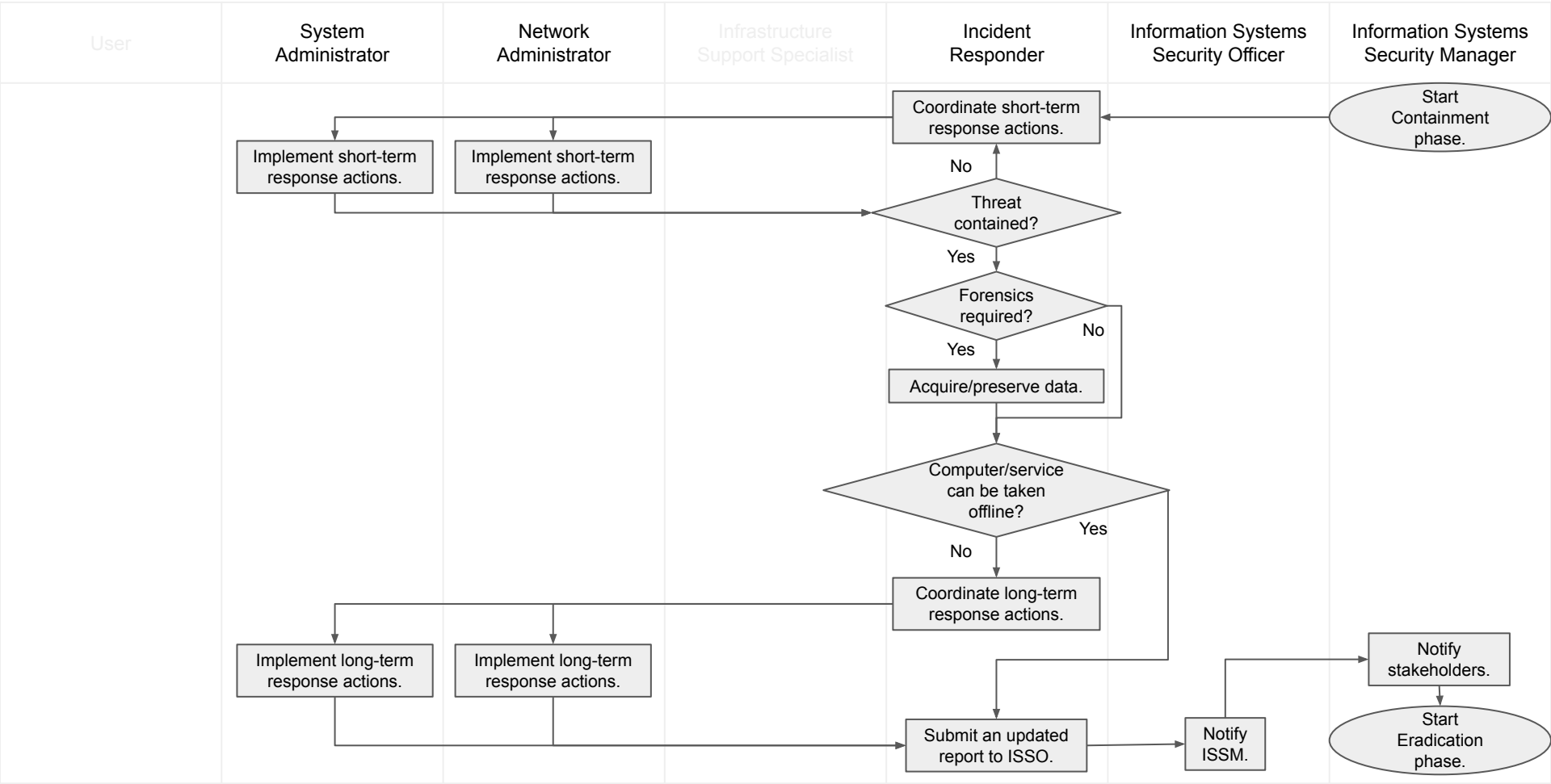


Incident Handling
Analysis Phase

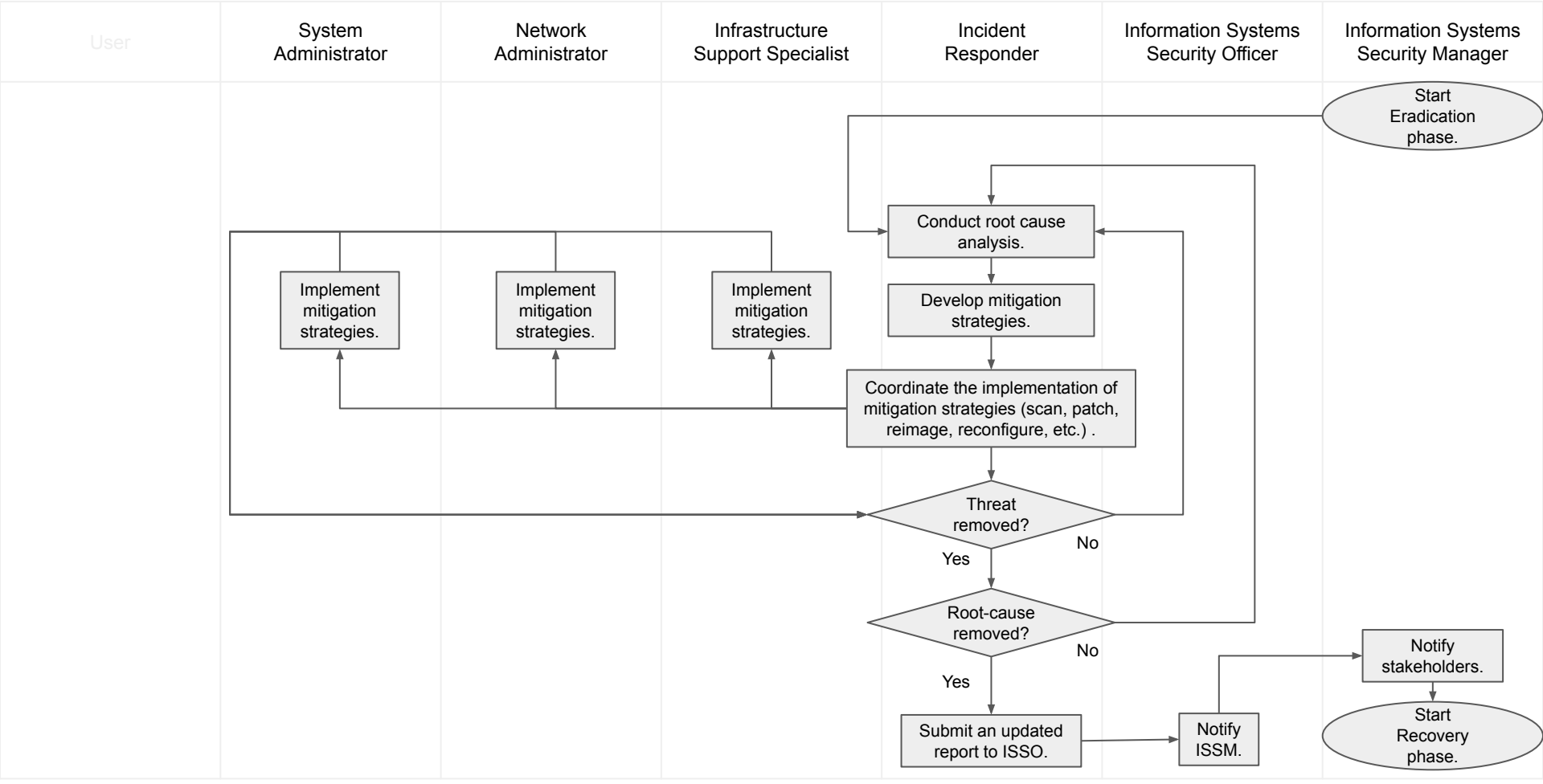
User	System Administrator	Network Administrator	Infrastructure Support Specialist	Incident Responder	Information Systems Security Officer	Information Systems Security Manager



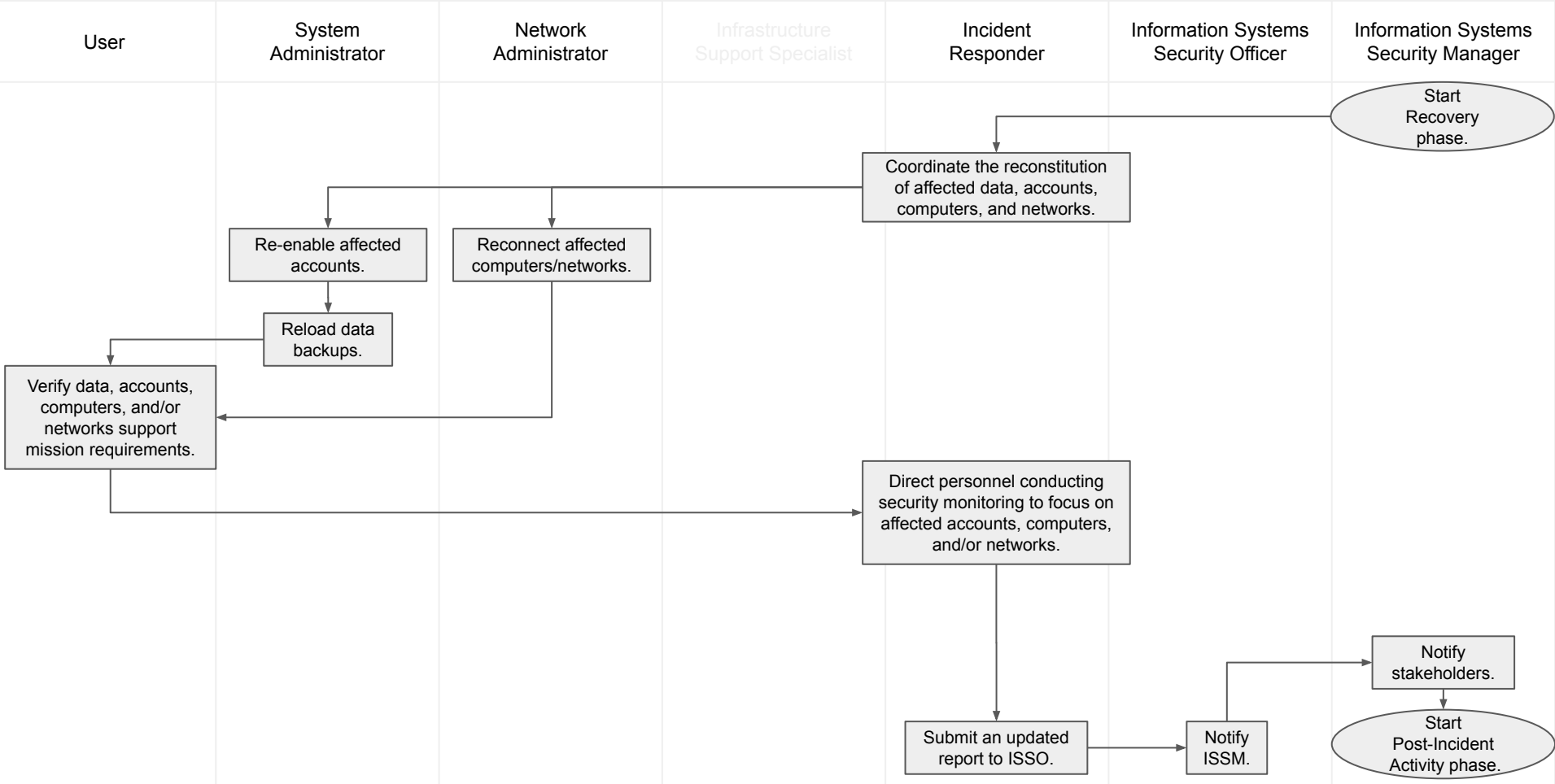
Incident Handling
Containment Phase



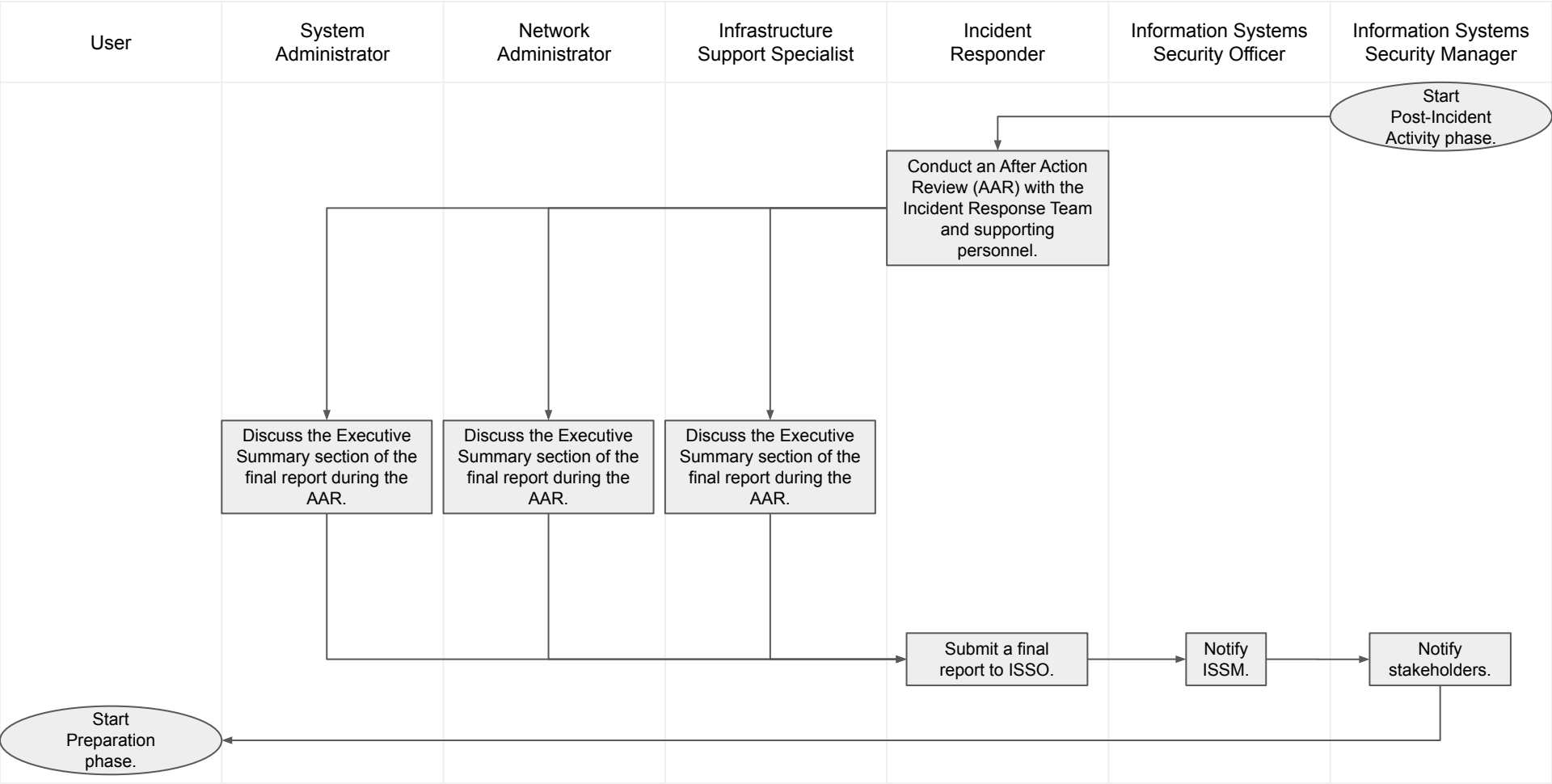
Incident Handling
Eradication Phase



Incident Handling
Recovery Phase



Incident Handling
Post-Incident Activity Phase



Incident Handling
Supporting Documents

Preparation Phase
- ❏ Duties and Responsibilities
- ❏ Security Requirements (Threat Model, DFD, AUP, etc.)
- ❏ Reportable Events and Incidents
- ❏ Reporting Templates
- ❏ Data Backup Policy and Procedures
- ❏ Asset Inventory
- ❏ Computer and Network Baselines
- ❏ Battle Rhythm

Detection Phase
- ❏ Incident Response Card
- ❏ Detection Playbook
- ❏ How to Create a Case File
- ❏ Initial Report Template

Analysis Phase
- ❏ CAT 1, 2, 3, 4, 5, 6, and 7 Investigation Cheat-Sheets
- ❏ Impact Assessment Cheat-Sheet
- ❏ How to Acquire and Preserve Forensic Evidence
- ❏ Chain of Custody Procedures

Containment Phase
- ❏ A Menu of Short-Term Response Actions
- ❏ A Menu of Long-Term Response Actions

Eradication Phase
- ❏ Root-Cause Analysis Guide
- ❏ A Menu of Mitigation Strategies

Recovery Phase
- ❏ Procedures for Reloading Data Backups

Post-Incident Activity Phase
- ❏ How to Conduct an AAR for Cyber Incidents

Threat Hunting
- ❏ Triggers
- ❏ Investigations
- ❏ Resolutions