{mthree}

Incident Management

Site Reliability Engineering

Overview

In this module, we will learn what an incident is, the primary roles and responsibilities during incident management and the key parts of incident response procedures.

Learning Objectives

- Define an incident
- Define incident management
- Managing incidents effectively
- Understanding the Enterprise Command Center
- Work through some incident identification and severity decisions

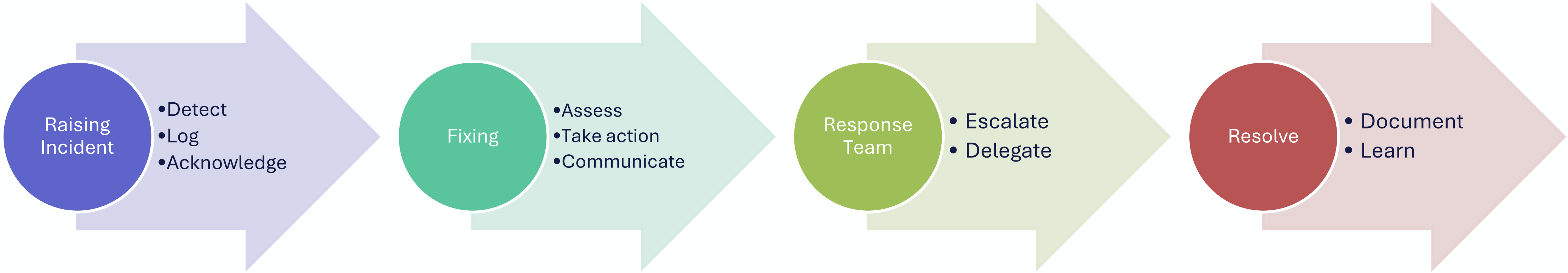
Student Incident Experience

- ↘ Overall experience with emergency/incident response
- ↘ Anticipated role(s) in responding to incidents

{mthree}

Introduction to Incident Management

- ↘ Describe placement of Incident Management within the normal operations
- ↘ Identify basic concept and benefits of an Incident Management plan



Raising Incident
- Detect
- Log
- Acknowledge

Fixing
- Assess
- Take action
- Communicate

Response Team
- Escalate
- Delegate

Resolve
- Document
- Learn

{mthree}

What Is an Incident?

An unplanned interruption of a service, or reduction in the quality of a service.
ITIL Foundation, ITIL 4 Edition ©AXELOS 2019

- Failure can occur at any time.
- It can take the form of:
  - Hardware failure
  - Software updates
  - Configuration changes
  - Accidental events
  - Malicious attacks

{mthree}

What Is an Incident Management Plan?

- Clearly describe the issue
- How detected or who manually triggered the incident
- Date and time the incident was reported
- Description of the incident
  - What is down
  - What is not working correctly
- Incident category
  - Helps locate possible fixes
  - Helps analyse trends, etc.
- Level of the incident

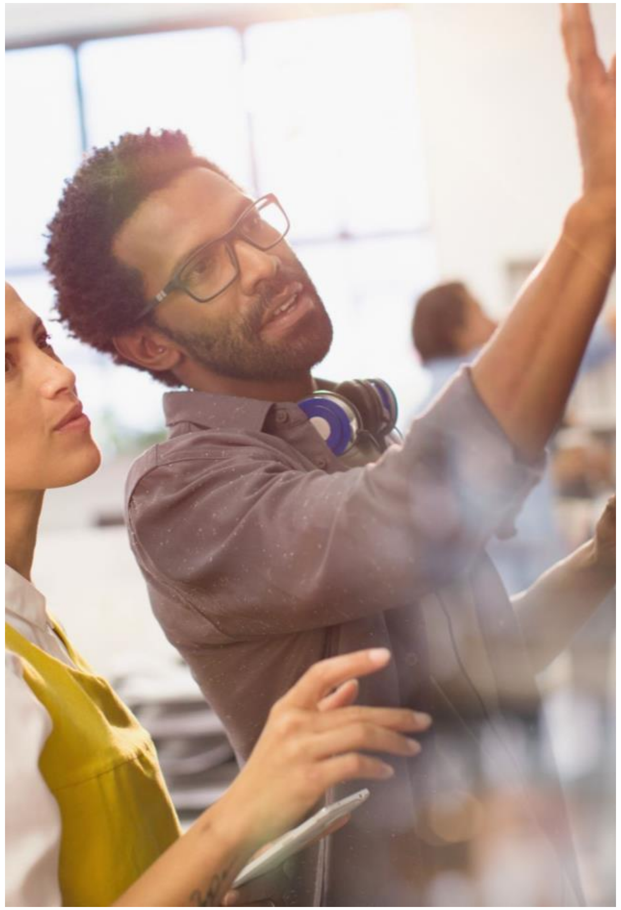
{mthree}

Levels of Incident

Severity Level	Description	Examples
SEV 1	A critical disruption to the business that requires public notification and coordination with the executive teams.	• Customer-facing service is down for all customers • Natural disaster has destroyed facilities disrupting business • Functionality is severely disrupted and is violating SLAs • Confidentiality or privacy is compromised, and customer is being exposed
SEV 2	A major incident with significant impact on customers' ability to use the service	• Customer-facing service is not available for a sub-set of customers • Core functionality is significantly impacted in the areas of performance or availability • System monitoring for major incident conditions is disrupted
SEV 3	A minor incident with low impact that require immediate attention	• Partial loss of functionality affecting a sub-set of the customers • Redundancy cluster down to one last node • Anything that has the likelihood of escalating to SEV 2
SEV 4	A minor issue with no impact on the customers' ability to use the service	• Performance degraded, but still at a usable level • Individual node failure in a cluster • Minor inconvenience to customers with a workaround available

What is Incident Management?

- A structured approach to incident response
- Adapted from Incident Command System
  - Used by emergency response organizations for natural disasters
  - Provides a clear and scalable process
  - Provides clear roles and responsibilities
- Enhances
  - Control
  - Coordination
  - Communication



{mthree}

Importance of Incident Management

- Major incidents are costly
  - $100000 - $300000 / hour or more
  - Loss of customer confidence
  - Regulatory penalties
- Well-defined and rehearsed Incident Management Process
  - Faster incident resolution (MTTR = Mean time to restore, repair, respond or recovery)
  - Reduced costs and/or revenue loss
  - Improved internal/external communications
  - Continuous improvement and learning

Incident Management Process

Communication

01

- Identify key roles and a clear chain of command

02

- Define responsibilities

03

- Capture response efforts for future analysis and learning

04

- Communicate response efforts

Benefits of Incident Management Planning

- Clearly defining a chain of command
- Everyone involved has a single person to report to
- Defined communications channels for clear and rapid communication
- Provide a systematic procedure to follow
    - Include flexibility to handle unique incidents
- Clear focus on the recovery of the business capabilities
    - While capturing data for continuous improvement

Making Incident Management Work

- Faster Incident Resolutions
  - < MTTR
- Reduced losses
- Improved communications
- Continuous Improvement
  - > MTTF
  - Learn from failures

{mthree}

Incident Action Planning

1

Cover a specified timeframe

2

Be proactive towards resolving

- Specify the incident objectives
- State the activities to be completed

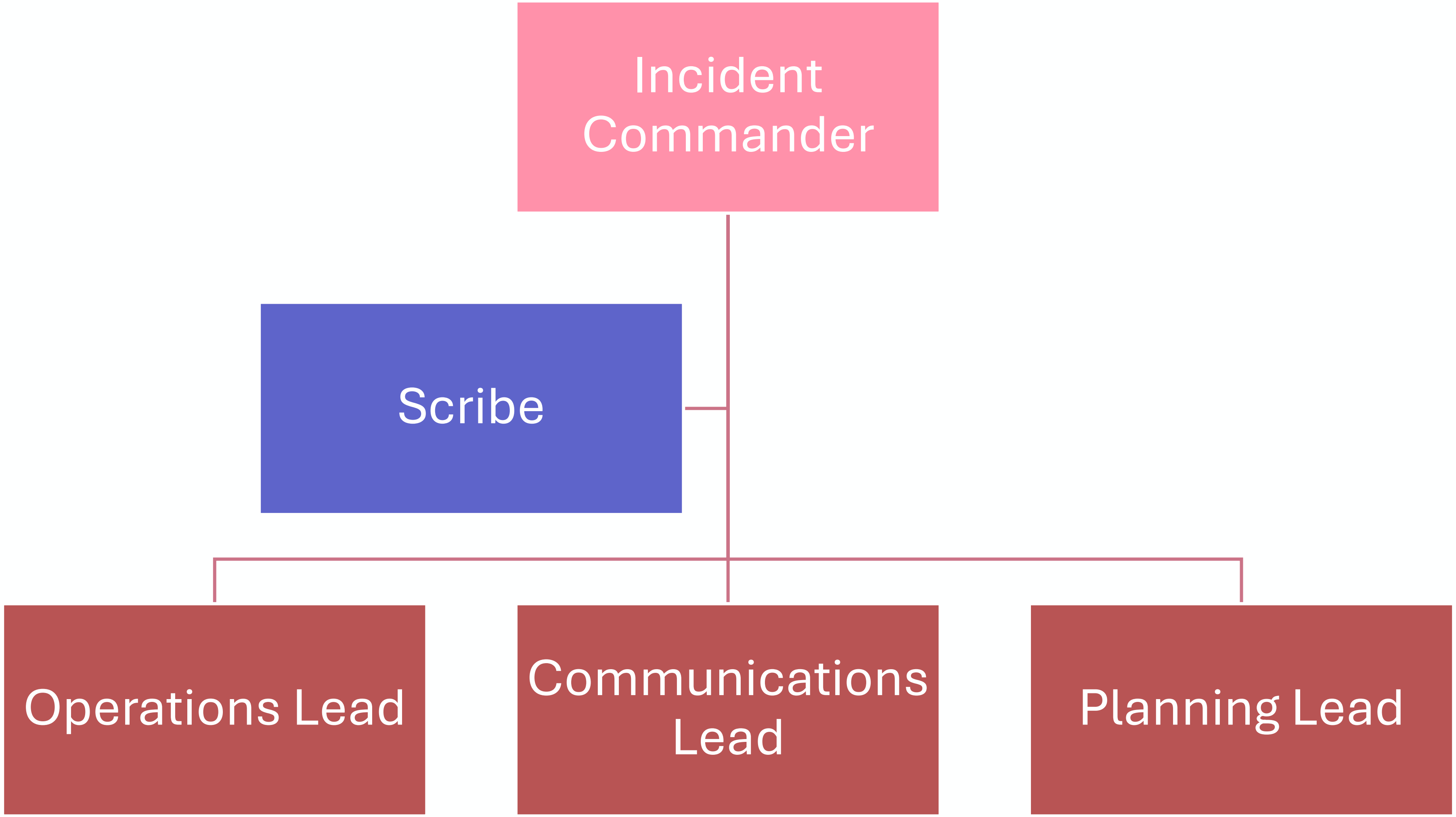
3

Assign responsibilities

- Identify needed resources

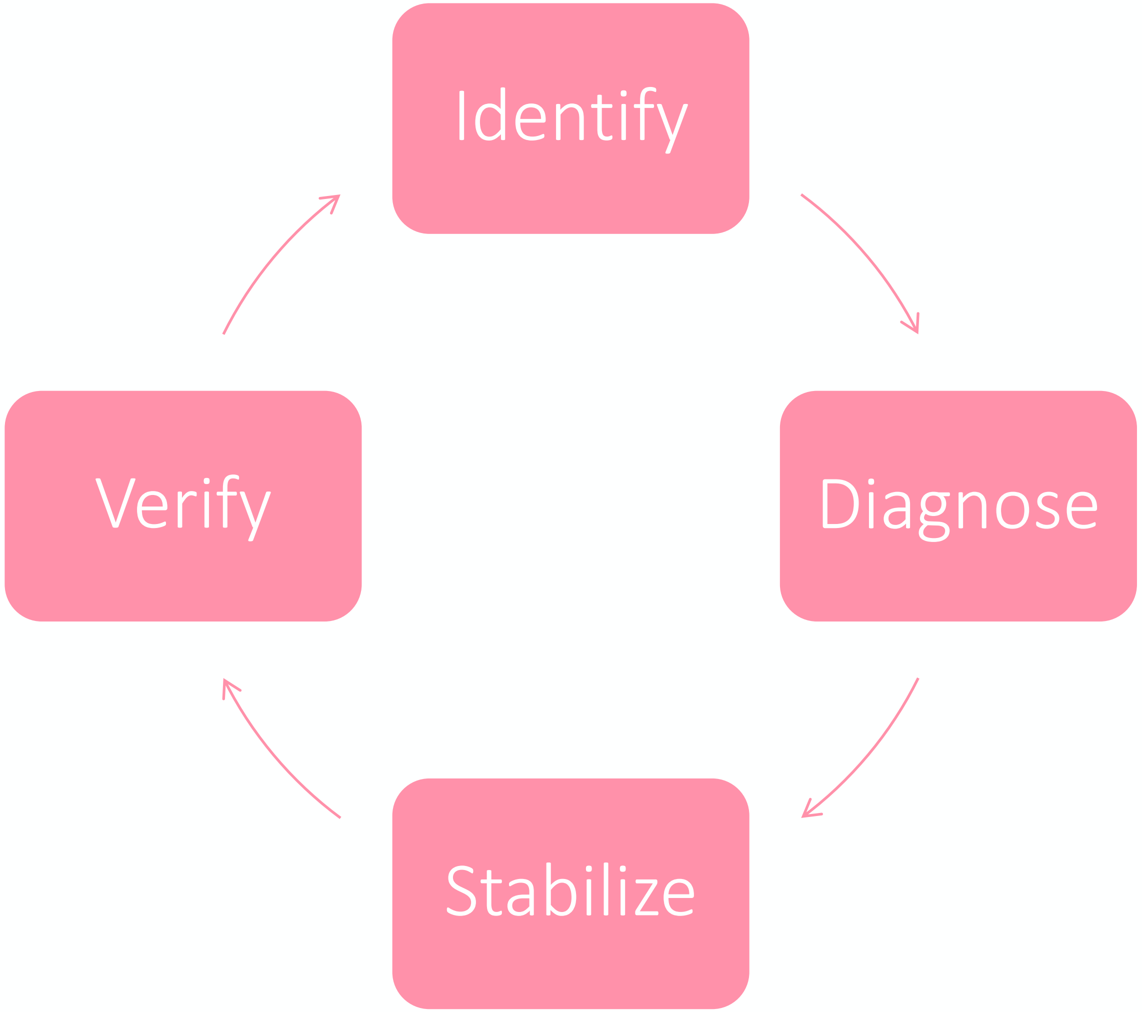
{mthree}

Incident Management Key Roles



{mthree}

Incident Cycle



{mthree}

Documentation

Do not leave this until later!

Accurate information is critical

- Don't rewrite it to make it look better

Critical to kept up to date and accurate

- Communication
- Post incident requirements for prevention

Summary
Q&A

References

- ↘ The Atlassian Incident Management Handbook
- ↘ Incident Response at Heroku 2020
- ↘ Google SRE - Managing Incidents
- ↘ Google SRE Workbook - Incident Management