{mthree}

Incident Management

Site Reliability Engineering

Objectives

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

{mthree}

Student Incident Experience

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

{mthree}

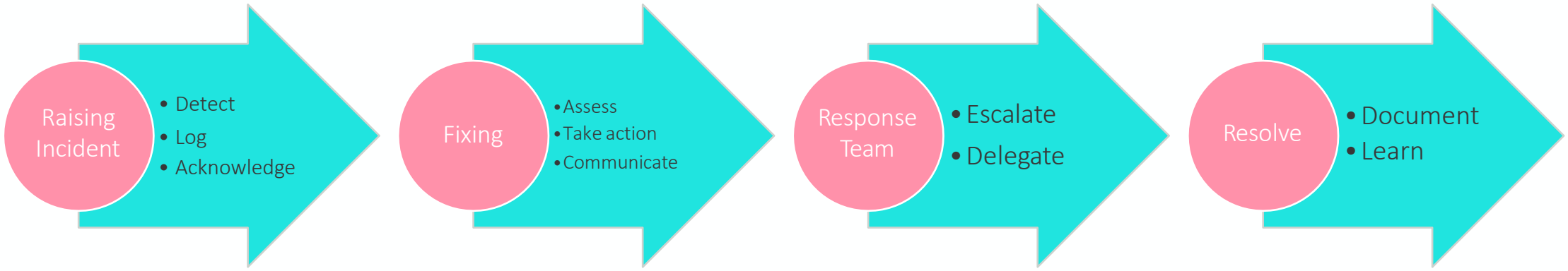
Student Expectations

What do you expect to gain from learning about incident management?

{mthree}

Introduction to Incident Management

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



{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

{mthree}

When an Incident Is Bigger Than the Team

Easy for multiple teams to be working redundantly or at cross purposes

Requires higher level of communication, control and coordination

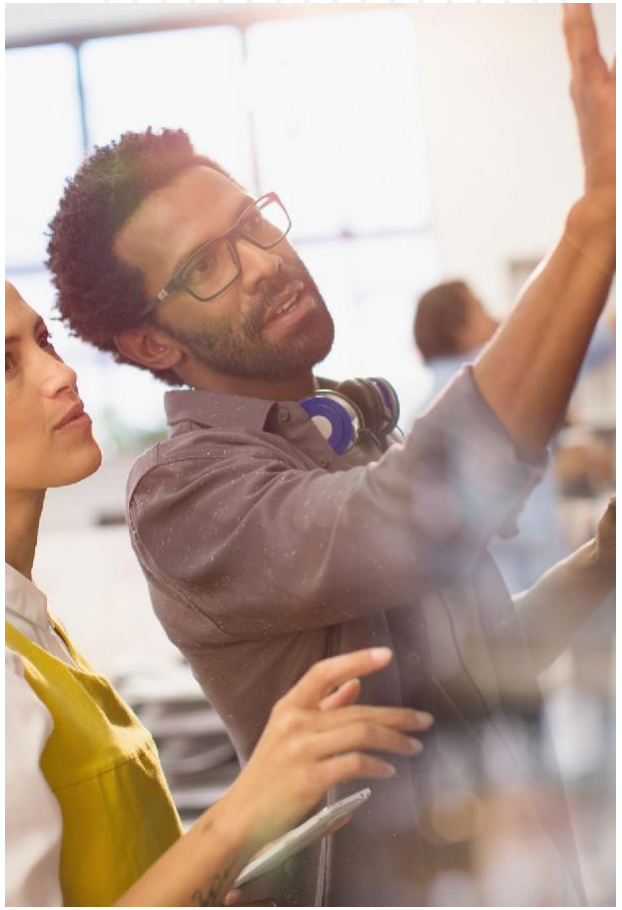
- Add additional members to the response team
- Escalate to experienced Incident Commander
- Escalate to Enterprise Command Center

Long-running incidents may also require handoff to teams across time zones as work progresses

{mthree}

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

{mthree}

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

{mthree}

Activity: Incident Management Benefits

- The purpose of this activity is to discuss the benefits of having an incident management plan and procedures in place before an incident occurs
- Divide into groups of 3 or 4
- Work as a team to review the scenario provided to you
- Come to a consensus as to the top three challenges in resolving this incident Capture your top three on a whiteboard
- Discuss amongst the team how an incident management plan could be used to address these challenges Select a spokesperson for your team
- Be prepared to report your team's findings back to the larger group.

{mthree}

Benefits of Incident Management Planning

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

Incident Management Characteristics

- Common Characteristics of Incident Management Plans
- Describe the common characteristics of needed in an Incident Management Plan

{mthree}

Making Incident Management Work

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

{mthree}

Characteristics Overview

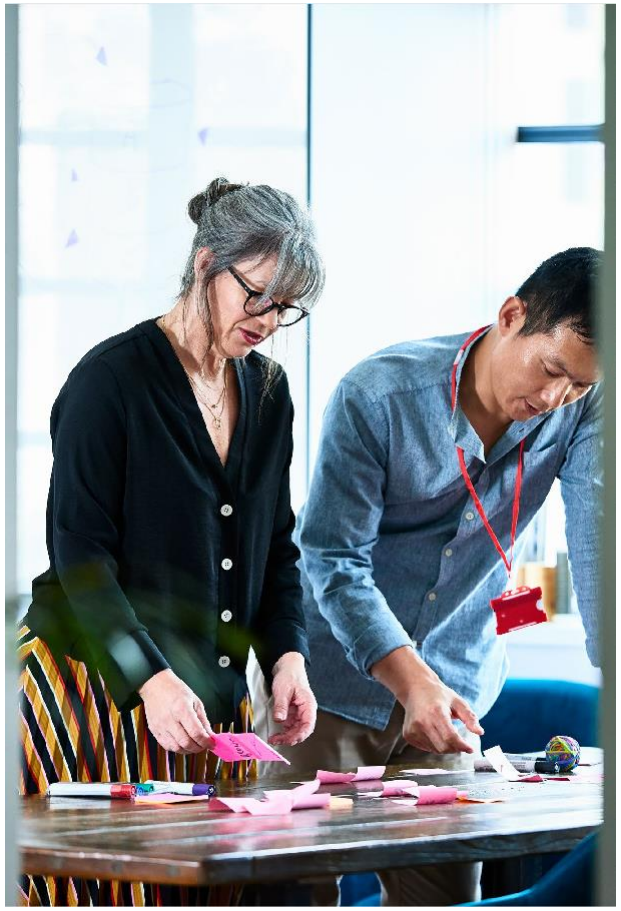
- Common Terminology
- Modular Organization Management by Objectives Incident Action Planning Manageable Span of Control Clear Communications
- Resource Management
- Command and Transfer of Command Clear Chain of Command
- Unity of Command Accountability

Common Terminology

- The response team likely has diverse backgrounds

  Use common terms

- Avoid
- Codes
- Acronyms
- Domain-specific language



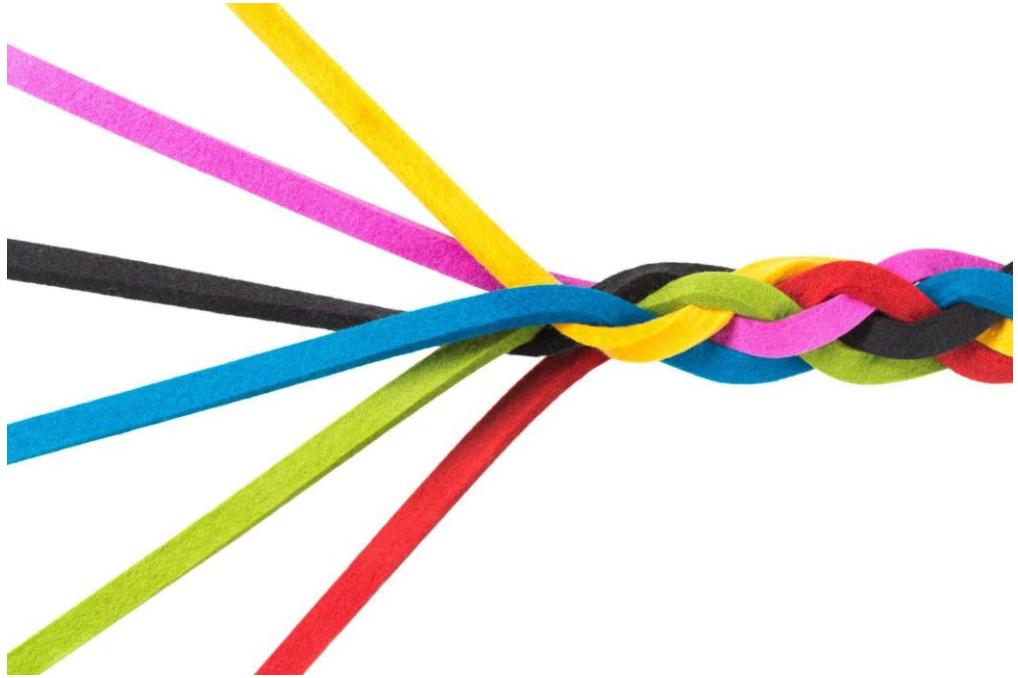
{mthree}

Common Terminology Discussion

- What codes, abbreviations, acronyms, etc., do you use when speaking with your colleagues?

Modular Organization

- Incident Commander can adjust as needed
- Increased complexity means responsibilities may need to be delegated
- Scribe
- Communications Lead
- Operations Lead
- Planning Lead



{mthree}

Management By Objectives

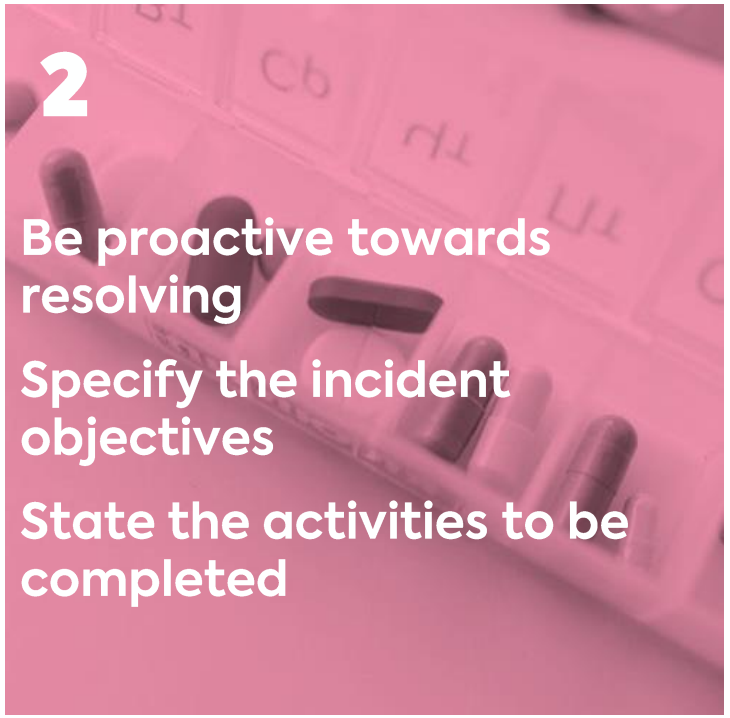
- Establish measurable objectives for the response
- Strategies Tactics Tasks Activities

- Issue assignments in a specific and timeboxed manner
- Specify who When

- Monitor the results of the incident tasks

{mthree}

Incident Action Planning



{mthree}

Incident Action Plan Questions

- Answer the following: What do we want to do?
- Who is responsible for doing it?
- How do we communicate with each other? What is the procedure if this makes it worse?

{mthree}

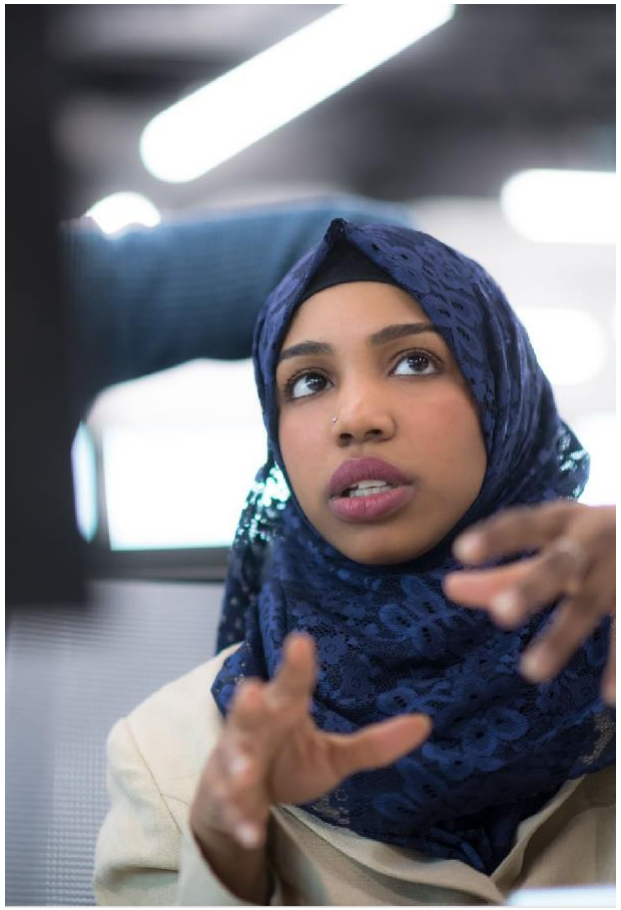
Activity: Incident Action Planning

- Purpose: To illustrate how to develop a plan Work in groups of 3 to 4
- Identify four items you would include in a plan for a provided scenario Identify tools that will be needed to manage the plan
- Capture these four items on a whiteboard
- Select a spokesperson to report back to the group
- Be prepared to share your answers in 5 minutes.

{mthree}

Manageable Span of Control

- Number of individuals directly leading
- Optimal ratio 1:5



{mthree}

Manageable Span of Control Discussion

- What are some examples of when span of control is most critical?

Clear Communications

- Possible solutions:
- Instant messaging channel
- Conferencing bridge or other audio/visual collaboration environment.
- Shared folders, SharePoint documents or other collaboration for documentation and information sharing.

{mthree}

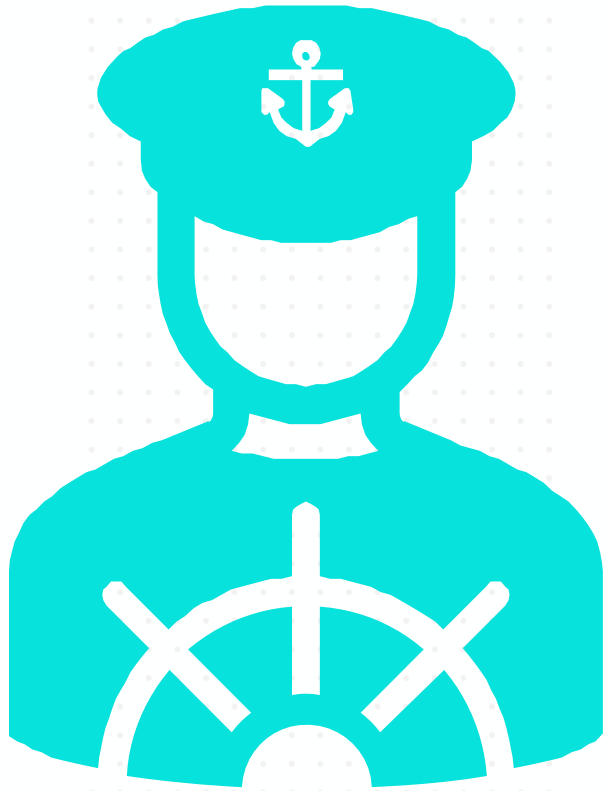
Resource Management

- Key resource management activities include:
  Resource identification
- Adding subject matter experts to the response team Planning for additional physical or cloud-based IT resources.

{mthree}

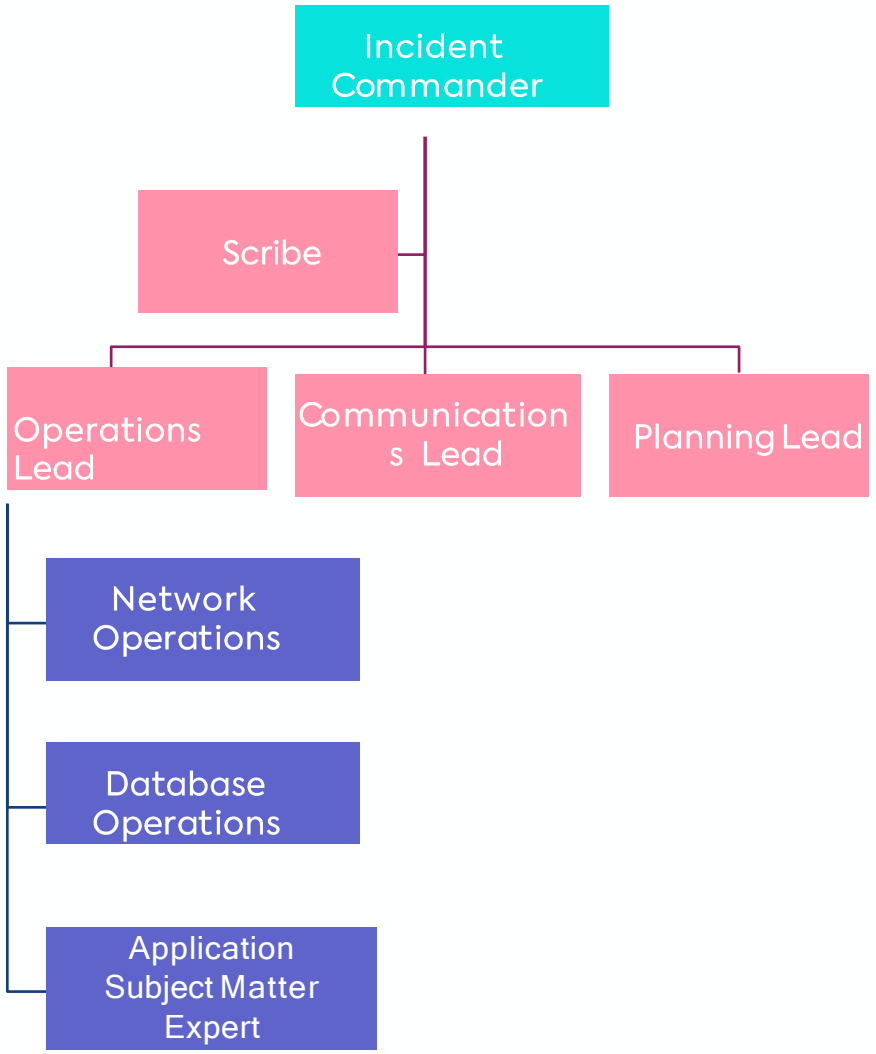
Establishing and Transferring Command

- Incident Commander is the first role filled Self-designated
- Assigned
- Relieving existing Incident Commander Expertise
- Endurance



{mthree}

Clear Chain of Command



{mthree}

Unity of Command

- Each team member has only one person to: Report to
- Receive assignments from

{mthree}

Accountability

- Clearly identify yourself and your role
- Response operations need to be coordinated as directed by the Incident Commander No heroic independent efforts
- Personal accountability for actions
- Track changes to the normal operations of the business Will likely need follow-up
- Span of Control monitored to adequately supervise areas

{mthree}

Functional Areas and Key Roles Overview

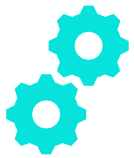
- Identify four major functional areas
- Describe the role of the Incident Commander
- Describe the select and transfer of command between Incident Commanders
  Identify roles associated with the response team
- Describe the roles of the response team

{mthree}

Functional Areas

Command

Communications



Operations

Planning

{mthree}

Functional Area Descriptions

- Incident Command
  Objectives
  Strategies
  Priorities
- Overall responsibility
- Communications
- Coordinates internal and external communications Formulates messages
- Updates communications channels
- Operations
- Arranges for resources and needed services
  Directs all operations resources
- Planning
- Tracking system changes
  Collecting/analysing information
  Documenting follow-up tasks

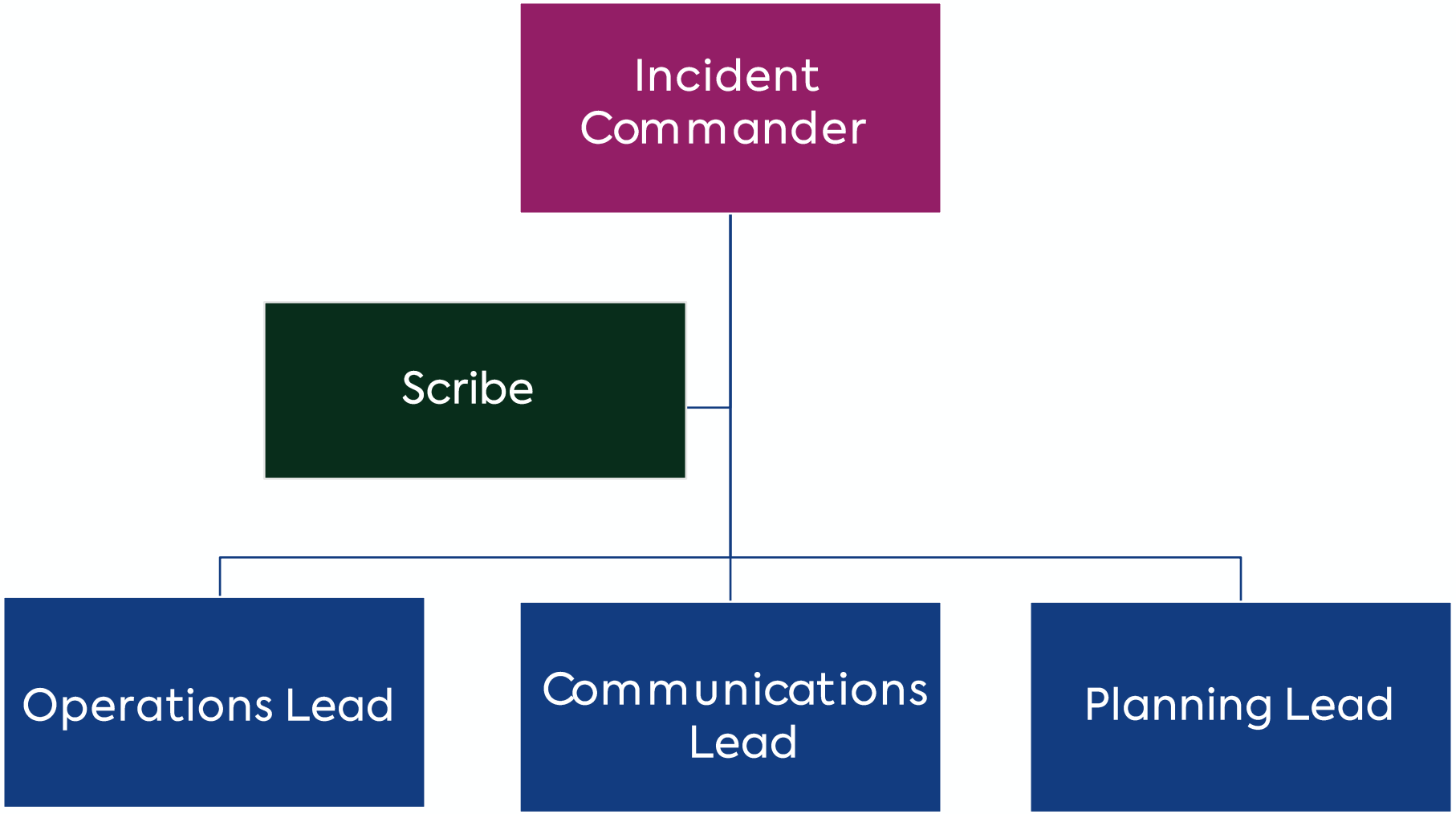
{mthree}

Review of Functional Areas

- Which functional area:
- Supports incident action planning process by tracking system changes, collecting/analysing information and documenting follow-up tasks that must be completed?
- Sets incident objectives, strategies, and priorities and has overall responsibility for the incident response?
- Conducts operations to reach the incident objectives. Establishes tactics. Arranges for resources and needed services and directs all operations resources?
- Coordinates internal and external communications, formulating messages and keeping frequent updates posted to the appropriate communications channels?

{mthree}

Incident Management Key Roles



{mthree}

Command Definition

- The act of directing, ordering, or controlling by virtue of explicit authority.
- Assists IC
- Captures communication
  Captures actions
- Captures discussion from conference bridge
- Use visible communication tool Chatroom (Slack/Teams/etc) Google docs
- Focus on capturing all information for future use

{mthree}

Incident Commander

- Responsible for overall coordination
- Keeps incident moving towards resolution
- Coordinates all the other roles
- De facto holder of any roles not delegated to others
- Delegates tasks
- Should not be personally making changes
- Only role always filled

{mthree}

Incident Command Discussion

- Why is it critical to establish command from the beginning of the incident?

Scribe Roles

- Assists IC
  - >>> Captures communication
  - >>> Captures actions
  - >>> Captures discussion from conference bridge
- Use visible communication tool
  - >>> Chatroom (Slack/Teams/etc)
  - >>> Google docs
- Focus on capturing all information for future use

{mthree}

Incident Commander Responsibilities

- Maintains documentation of incident
- Critical to keep track of what has already been done Necessary for lessons learned analysis
- Can delegate to Scribe
- Ensuring the overall stability of the system throughout the response
- Providing information to internal and external stakeholders, such as the executive suites, customers, and regulatory agencies
- Establishing and maintaining liaison with third-party and oversight agencies participating in the incident response

{mthree}

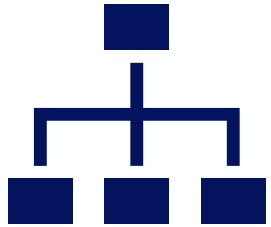
Selecting or Changing Incident Commanders

- Selecting
- Self-designated initial Incident Commander Incident Commander On Call Changing
- Qualified Incident Commander assumes command (e.g., the individual who discovered the incident accepts the Incident Commander role until an on-call Incident Commander can join the response team)
- Incident changes in complexity.
- The current Incident Commander needs to rest, on long or extended incident this may require a rotation be established.
- The organization is set up to follow the sun through different time zones and the end of the current workday is approaching.

{mthree}

Transfer of Command Discussion

- Always include a thorough transfer of command briefing

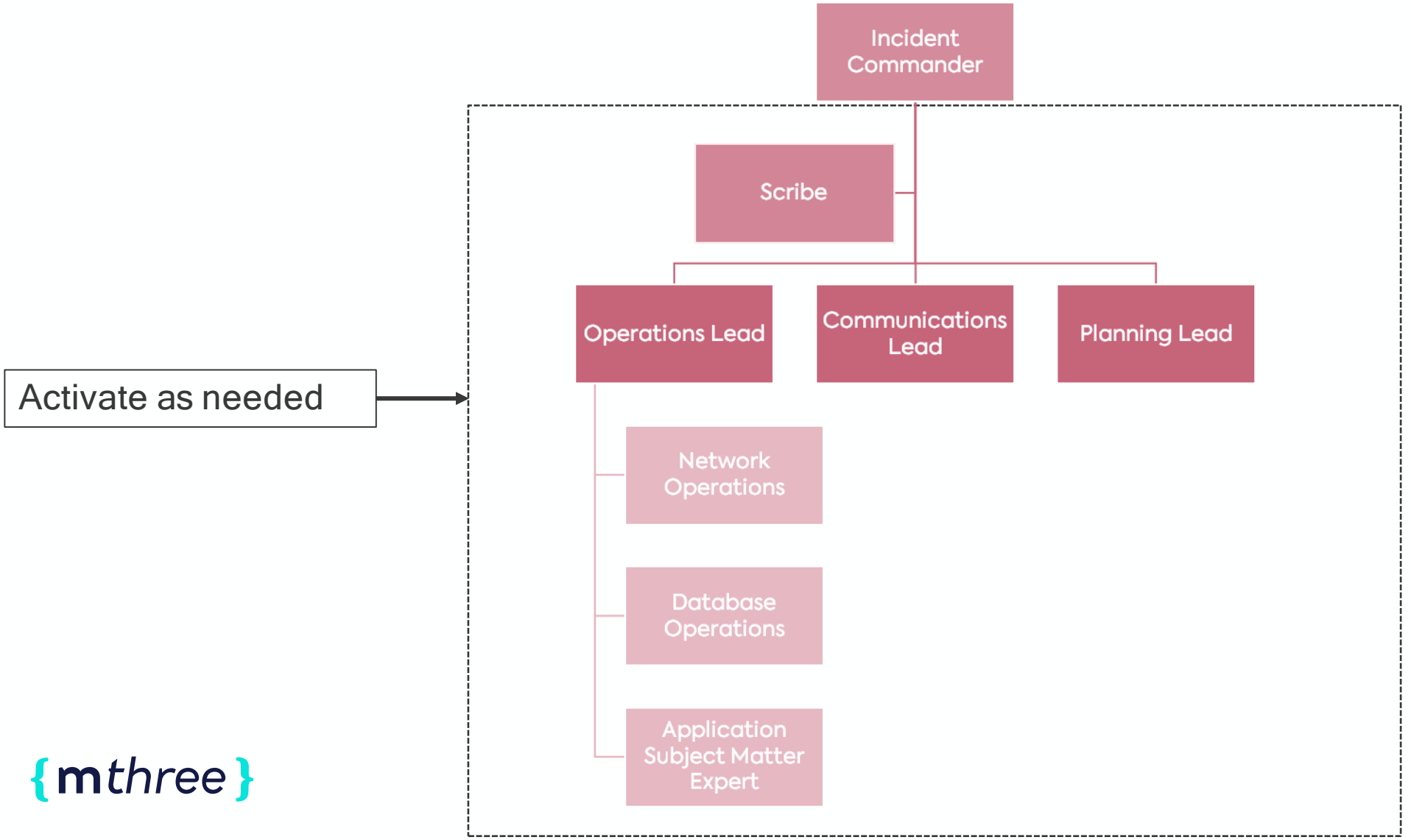


- Notify the rest of the incident response team

- What would you include in a transfer of command briefing?

{mthree}

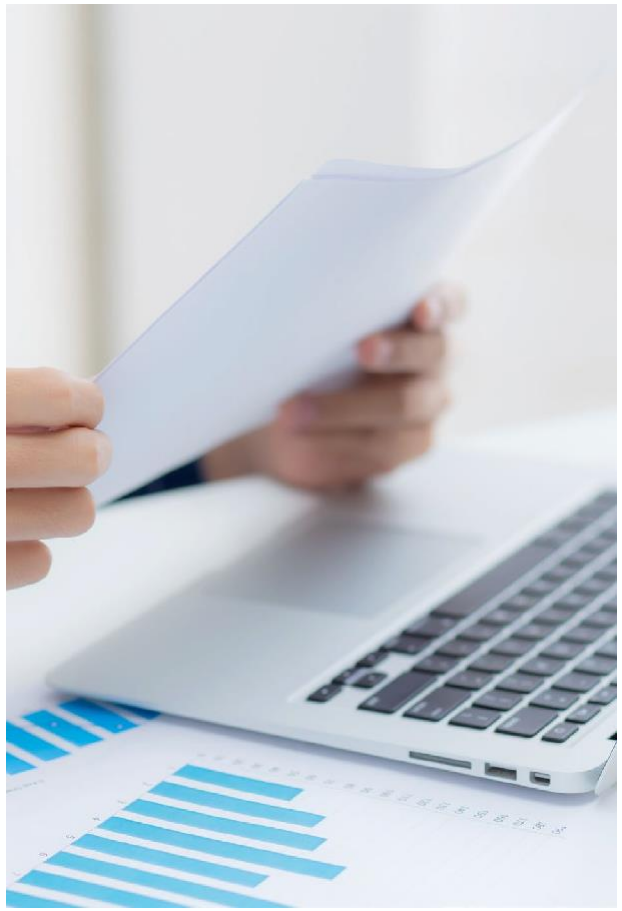
Delegating Incident Management Responsibilities



{mthree}

Scribe

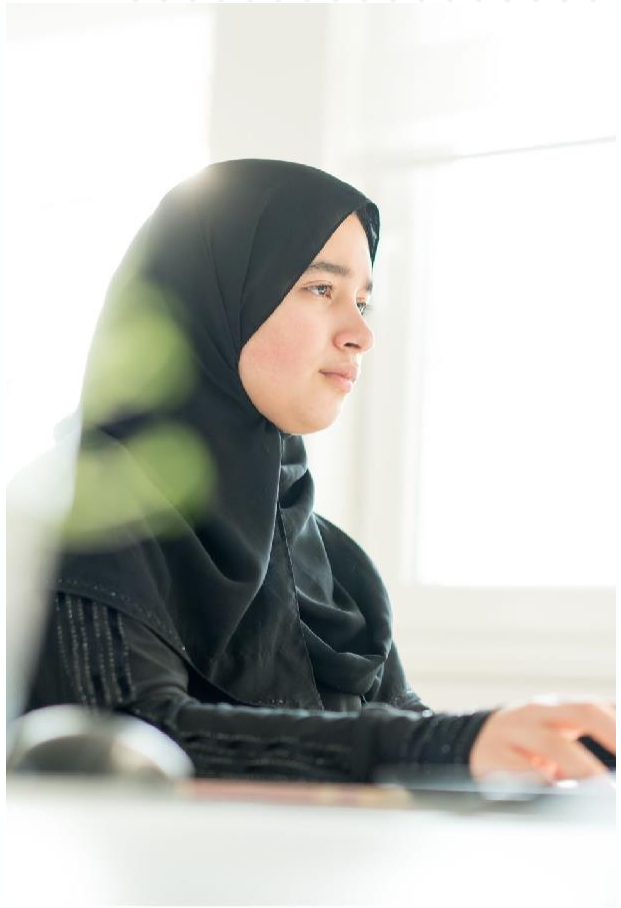
- Critical importance of capturing information During the incident response efforts
- Sufficient detail to allow analysis of the response during postmortem Should not be sanitized
- Not edited to make the response appear better



{mthree}

Operations Lead

- Works with the IC
- Develop theories about what is broken and why Recommend changes to the IC
- Coordinate the operation team's efforts to restore the service
- Makes sure changes are made in a controlled manner
- Makes sure that only operation teams are making changes to the system Brings in subject matter experts (SMEs) to assist



{mthree}

Communications Lead

- Communications are critical Internal
- External
- Periodic updates Status page
  Social media
- Direct communication
- May be delegated to maintain incident documentation
  Communication
- Post incident analysis

{mthree}

Planning Lead

- Supports OL and IC Capturing long-term issues Creating tickets
- Arranging handoffs
- Tracking system divergence from SLO
- Supporting Operations teams Ordering food

{mthree}

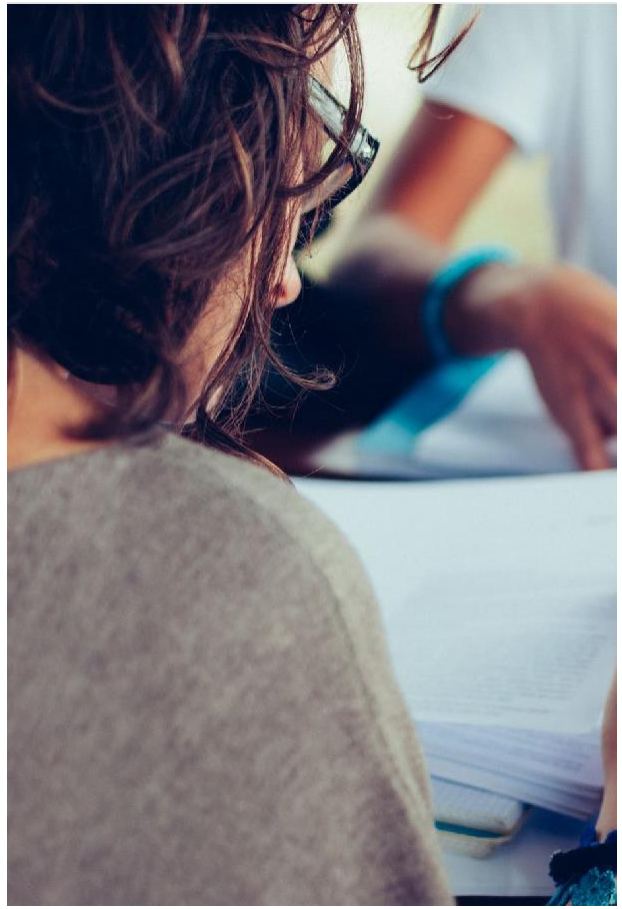
Staff Review

- Name the staff member described below:
- As the response is underway, my area tracks changes made to the system in anticipation of a need to restore the configuration after the incident.
- As the response progresses, my area manages the communication with internal stakeholders, customers, and other interested parties.
- As the incident unfolds, I capture the events, plans, discussions and results for communications and postmortem analysis.
- During the response, my area is responsible for implementing strategies and developing tactics to carry out the incident objectives.

{mthree}

Service-Specific Subject Matter Expert (SME)

- Called in to advise on service-specific knowledge
- May not normally be involved in operations



{mthree}

SME On-Call Responsibilities

- Familiarize yourself with the other roles
- Join the incident communications channel ASAP Offer theories and suggests
- Support decisions are made by the Incident Commander Keep focus on resolving the incident
- Leave the incident channel when asked

{mthree}

Backup SME

- Should be call list for service-specific SME
  - May be unavailable

Managing Incidents Effectively

Know when to deal with an incident

Identify impacts

Understand incident management behavior

{mthree}

When to deal with an incident

- Requires immediate and dedicated effort to resolve Determine incident level and impact
- Deal with incident ASAP when
- SLI indicates current or imminent failure to meet SLO Customer complaint
- Declare incident immediately, unless the fix is obvious and easy

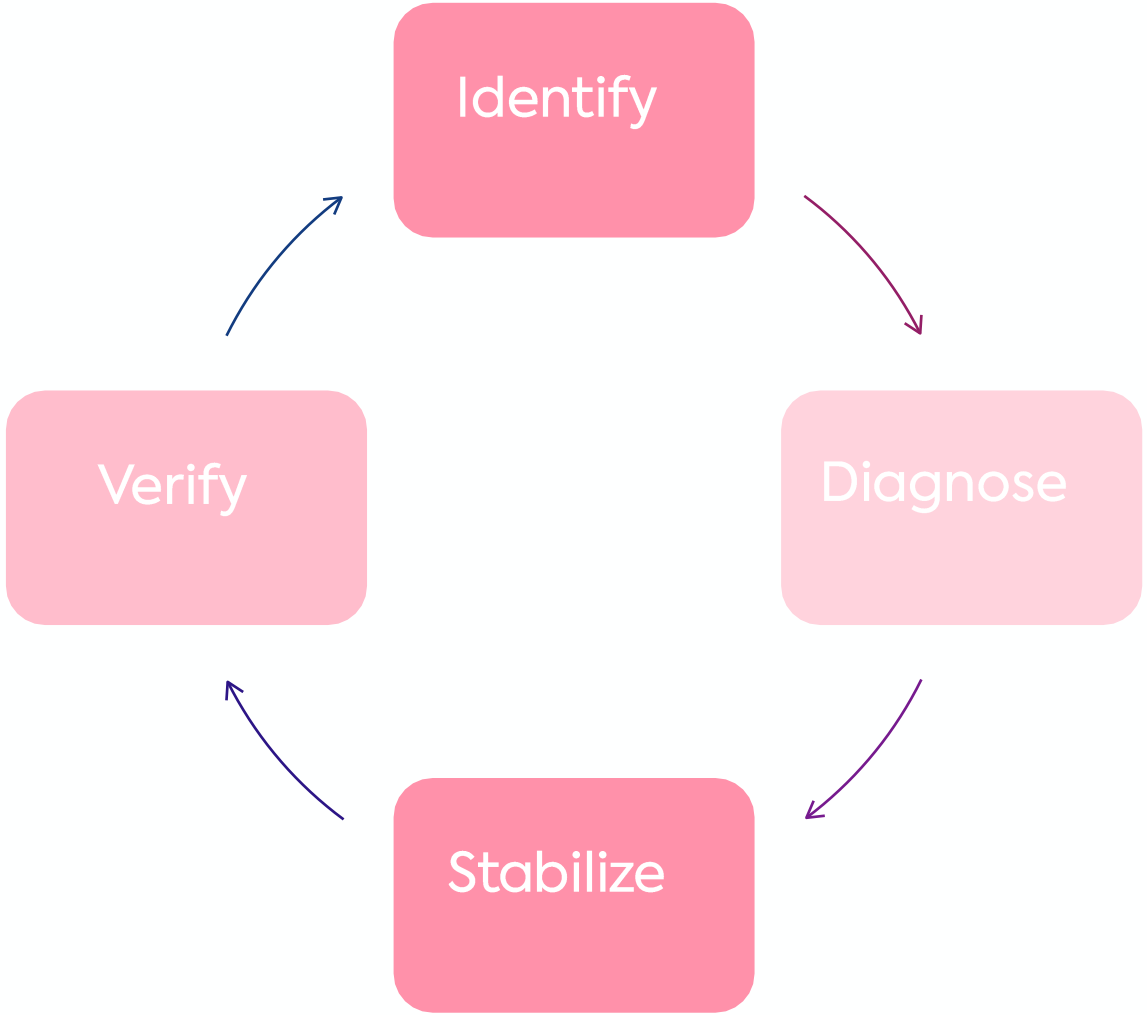
{mthree}

Identifying impacts

- Who and how many are impacted
- Service unavailable
- Consider dependencies
- SLO/SLA in violation
- Or likely to be soon
- Monetary
- Loss of income
- Penalties
- Fines
- Regulatory
- Legal risk
- Loss of license/permit to operate
- Criminal risk

{mthree}

Incident Cycle



{mthree}

Incident Management Checklist

- Acknowledge the incident
- Initialize internal and external communications channels
- Research the issue
- Triage for scope and severity Make an initial diagnosis
- Localized or other systems impacted Dependencies
- Fixable/Escalate
- Check for existing playbook to handle Is a fix automated already
- Identify who is needed to fix Estimate scope in time and resources Gather information
- To assist the next level when escalated
- To be reviewed in the postmortem
- Root cause analysis
  Document
- Follow-up task tickets
- Close the incident

{mthree}

Incident Response Behaviour

- May deviate from normal operations
- Normal seniority is not applied Response team is ultimate authority Incident Command
- Consensus when can
- Decisive always
- Tensions are high
- Do not take it personally

{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

{mthree}

Closing the Incident

- Communicate, communicate, communicate!!!
- Ensure that the person who filed the incident is satisfied that it is fixed
- Preventive measures
- What cause(s) can be eliminated
- Key indicators to monitor
- Prevention or early notice of future incidents
- Documentation needs to be available for future reference Good reference to future incidents
- Postmortem – what was learned
  Covered in the next module

{mthree}

Enterprise Command Center (ECC)

- Why are we here?
- Do we have everyone we need? What's the problem?
- What can't they do?
- What's been identified?
- What fixes are recommended? Coordination of fix
- Are we working?
- Does everyone know what they did and when?

{mthree}

Discussion – Why Escalate to Enterprise Command Center?

- Instructor will break you into groups of 3–4.
- Discuss why there could be benefits in escalating an incident to an Enterprise Command Center. Select a spokesperson to report back after 5 minutes.

{mthree}

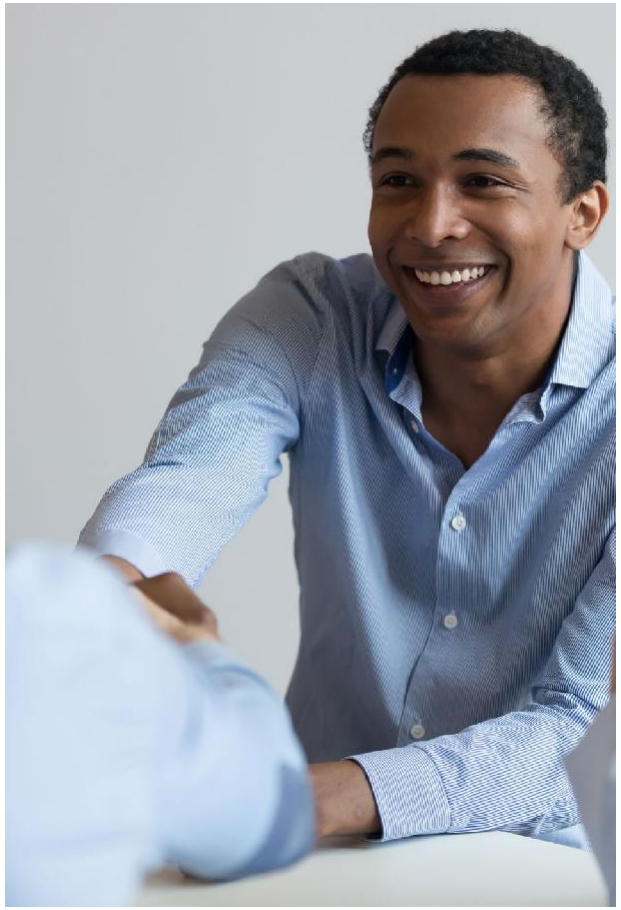
Benefits of Unified Command

- Unified efforts
- Across multiple teams
- One voice in communicating
- Customers
- Public
- Executives Emphasized urgency
- Handle conflicting goals

{mthree}

Incident Commander Role Changes

- Reduced Enterprise Authority Resides with ECC
- Assists in Strategic Planning
- No longer responsible for strategy
- Communication to ECC



{mthree}

Activity – Incident Management Practice

- In this activity we want you to: Identify the incident Determine incident level
- Does it require ECC intervention?
- What other teams might need to be involved? What fix might work?
- Explain the reasoning behind your suggested actions.
- Test the fix
- Record results
- Capture response timeline.

{mthree}

Summary
Q&A

{mthree}

References

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