Incident Management

Incident management involves the activities an organization performs to identify, analyze, and correct operational events that cause unplanned interruptions and service outages. The key objectives are to:

- Restore service operations as quickly as possible
- Minimize adverse impacts to the business and customers
- Maintain service levels by rapidly resolving incidents

An incident is an unplanned interruption that reduces the quality of an IT service or business process. Incidents require immediate response to mitigate impacts. Examples include system crashes, network outages, cyber attacks, supply chain disruptions, etc.

When an incident occurs, the following key steps are performed:

- Detection - Monitoring systems trigger alerts or users report issues
- Logging - Create an incident report with details like date, impact, urgency, etc.
- Categorization - Assign incident type, priority, and route accordingly
- Diagnosis - Investigate and determine likely root cause(s)
- Resolution - Take actions to restore normal operations and mitigate impact
- Recovery - Confirm resolution fixed the underlying problem
- Closure - Document lessons learned and required improvements

A structured approach to incident management detects issues early, minimizes recovery time, and identifies ways to prevent recurrences. Post-incident analysis using techniques like 5 Whys root cause analysis can uncover process weaknesses.

Effective incident management requires planning and practice. Teams should be trained, roles defined, backups identified, and response procedures established pre-crisis. Proper escalation protocols and communication plans need to activate when incidents strike. With a strong incident management capability, organizations can maintain critical services and bounce back quicker.