PRADITA University

MTI104 - IT Services

Session-10:

Practices to Manage Changes

PRU/SPMI/FR-BM-18/0222

Alfa Yohannis

The Heart of ITIL

PRADITA University

- ITIL's core lies in operations.
- Value is created or lost in this phase.
- Customers' experiences shape their perceptions.
- Enhancements or developments may pause, but operations continue.
- Operations persist until the product's end of support or service is active.
- Operations are crucial for organizational success.

The Role of Operations

PRADITA University

- Most action occurs during operations.
- Customers remember interactions during this phase.
- Service providers bill the most during operations.
- Operations are not the best place to invest heavily.
- The significance of operations will be explained further.

Operational Activities

PRADITA University

- Focus on maintaining products and services.
- No functional or nonfunctional modifications are made.
- Status quo is maintained to ensure service consistency.
- Operations run the longest and involve the most staff.
- Customer perception is formed through operational achievements.

Challenges in Operations

PRADITA University

- Strategies and designs may change over time.
- Technological innovations bring changes.
- Transitions and training may lead to support glitches.
- DevOps simplifies product and service maintenance.

Job Security and Trends

PRADITA University

- Operations roles offer job security.
- Flexibility is needed to adapt to organizational needs.
- DevOps professionals manage CI-CD tools and coding.
- Multiple skills are crucial for survival in the IT industry.

Practices in Operations

PRADITA University

- Monitoring and Event Management
- Incident Management
- Problem Management
- Important for ITIL Foundation exam.
- Focus on understanding these practices in depth.

Monitoring and Event Management

PRADITA University

- Systematically observe services and components.
- Record and report selected changes of state (events).
- Detect problems early to minimize service outages.
- Monitor critical Configuration Items (CIs).

Types of Events

PRADITA University

- Exception Events: Indicate errors, require urgent action.
- Warning Events: Indicate potential issues, need caution.
- Informational Events: Convey status changes, no urgent action required.

Key Activities in Monitoring

PRADITA University

- Develop monitoring strategies and designs.
- Define thresholds for warning and exception events.
- Implement monitoring tools and processes.
- Automation is crucial for effective monitoring.

Incident Management Practice

PRADITA University

- Deals with unplanned service interruptions.
- Affects customer satisfaction and service quality.
- Reacts to situations; efficiency depends on speed of resolution.
- Common in ITIL and critical for managing service disruptions.

Incident management life cycle

PRADITA University

Definition of an Incident

PRADITA University

- Unplanned interruption to a service or reduction in quality.
- Examples: Netflix buffering, email issues, hard drive failure.
- The goal is to restore service and minimize disruption.

Introduction to Incident Management

- An incident is a disruption to a service.
- Incidents are common but undesirable.
- Goal: Minimize incident rate and lifespan.
- Minimized downtime = Increased customer satisfaction.
- Focus: Quick resolution of incidents.
- Example: Netflix buffering vs. playing movie quickly.
- Time is essential in incident resolution.

Incident Management Practice

PRADITA University

- Proactive vs. Reactive: Incident management is reactive.
- Importance: Reducing impact through quick resolution.
- Incidents are unavoidable; managing them is crucial.
- Compare to sickness: Find cure (fix) and preventive measures (immunity).
- Manage downtime to be minimal.
- Improvements like auto-reindexing to prevent issues.

Incident Management Practices

PRADITA University

- Log all incidents, including internal staff findings.
- Implement self-help tools for hands-free operations.
- Have a capable service desk as the first contact.
- Establish a functional escalation matrix.
- Maintain a matrix of responsible teams for incidents.
- Involve all stakeholders in incident resolution.
- Build specialized teams for critical incidents.

Good Practices in Incident Management

- Use swarming techniques for initial resolution stages.
- Address service continuity through disaster recovery plans.
- Record all updates on an incident register.
- Service continuity management ensures service endures during disasters.
- Techniques: Data replication, disaster recovery, resilience building.

Incident Management Life Cycle

PRADITA University

- Various incidents need standardized management.
- Life cycle steps can vary by implementation.
- Example steps:
  1. Incident Identification
  2. Incident Logging
  3. Incident Categorization
  4. Incident Prioritization and Investigation
  5. Diagnosis
  6. Resolution
  7. Incident Closure

Incident Identification

PRADITA University

- Incidents must be identified via triggers.
- Common triggers:
  - Monitoring and Event Management
  - Telephone
  - Email/Chat
  - Web Interface
- Importance of identifying and managing triggers.

Incident Logging

PRADITA University

- Log all identified incidents with timestamps.
- Use ITSM tools like ServiceNow, BMC Remedy.
- Common fields on incident tickets:
  - Incident number, End user name, Time of logging
  - Impact, Urgency, Priority, Category
  - Incident summary, Assigned resolver group

Incident Categorization

PRADITA University

- Categorize incidents into appropriate buckets.
- Correct categorization is crucial for effective resolution.
- Example: Network issue vs. application issue.
- Autologged and user-raised incidents may require careful categorization.

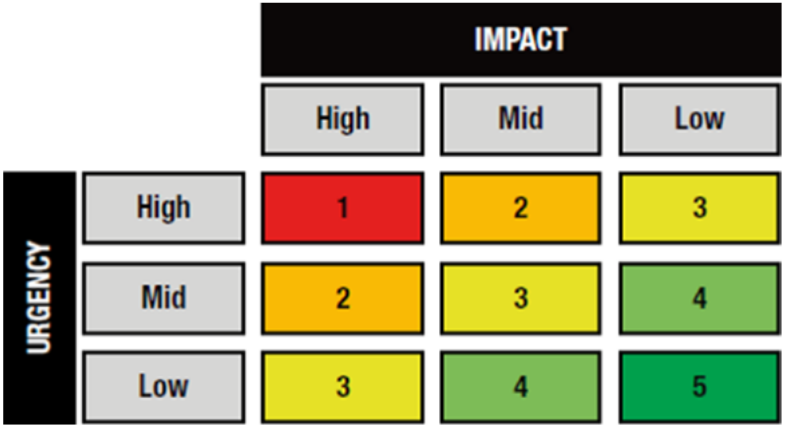
Incident Prioritization

PRADITA University

- Prioritization based on impact and urgency.
- Examples:
  - Major impact and urgent = High priority
  - Minor impact and non-urgent = Low priority
- Priority determined by a matrix.
- Response SLA and Resolution SLA are defined.

Incident priority matrix

PRADITA University



Incident Priorities and SLAs

PRADITA University

- Incident priorities may change during the life cycle.
- Response SLA: Time to acknowledge the incident.
- Resolution SLA: Time to resolve the incident.
- Example: P1 priority with 15-minute response and 2-hour resolution.
- SLAs vary by customer requirements and incident priority.

Incident management SLAs

PRADITA University

Response and Resolution SLAs for Incidents		
Incident Priority	Response SLA	Resolution SLA
P1	15 minutes	2 hours
P2	45 minutes	6 hours
P3	2 hours	1 day
P4	1 day	3 days

Step 5: Diagnosis and Investigation

PRADITA University

- Initial diagnosis by understanding symptoms
- Identify what's not working
- Basic troubleshooting steps
- Analogous to a doctor asking about symptoms
- Key substep providing data for further investigation
- Service desk may escalate to level 2 (L2) support
- L2 groups: server, network, storage, or software experts

Step 5: Diagnosis and Investigation (cont.)

- Resolver group uses available information
- May call user for more details
- Incorrect questioning may lead to starting over
- Investigation involves:
  - User expectations
  - What went wrong
  - Sequence of steps
  - Impact and scope
  - Recent changes
  - Similar incidents or KEDB articles

Step 6: Resolution and Recovery

PRADITA University

- Apply resolutions based on investigation
- Troubleshoot at appropriate level (server or network)
- Success depends on correct investigation path
- Tests and recovery period for widespread incidents
- Major incidents may remain open for observation
- Daily/hourly meetings with stakeholders

Step 7: Incident Closure

PRADITA University

- Confirm with user before closing ticket
- Service desk handles confirmation
- Alternative: Incident remains resolved for 3 days
- Email to user for confirmation
- Autoclosure if no response
- User satisfaction survey post-closure

Major Incident Management

PRADITA University

- Major incidents: High impact and potential damage
- Separate process with stringent timelines
- Major incident managers handle these incidents
- High pressure and responsibility
- Separate team and specialized skill sets
- Communication and updates to all stakeholders

Engagement with Service Value Chain

ADITA iversity

- Plan: Low involvement in incident management
- Design and Transition: Medium involvement
- Obtain/Build: Medium involvement
- Engage: High involvement
- Deliver and Support: High involvement
- Improve: Medium involvement

Problem Management Practice

PRADITA University

- Incident management: Immediate relief
- Problem management: Long-term prevention
- Focus on root causes of incidents
- Problem management as the ”CSI” of IT
- Example: Application crash and resolution
- Prevention through problem management

ITIL Definition of Problem

PRADITA University

- Cause or potential cause of incidents
- Unresolved incidents until root cause is known
- Avoiding guesswork in solutions
- Example: Doctor prescribing without diagnosis
- Problem management seeks root causes

Incidents vs. Problems

PRADITA University

- Incidents: Loss or degradation of services
- Problems: Root causes of incidents
- Problems arise when root cause is unknown
- Example: Software application crash
- Problem management for permanent solutions

Other Key Terminologies in Problem Managem

- Root Cause: Fundamental reason for an incident
- Root-Cause Analysis (RCA): Techniques to find root cause
- Known Error: Analyzed problem with no permanent fix
- Known Error Database (KEDB): Repository of known errors
- Workaround: Temporary fix for incidents
- Permanent Solution: Long-term resolution of root cause

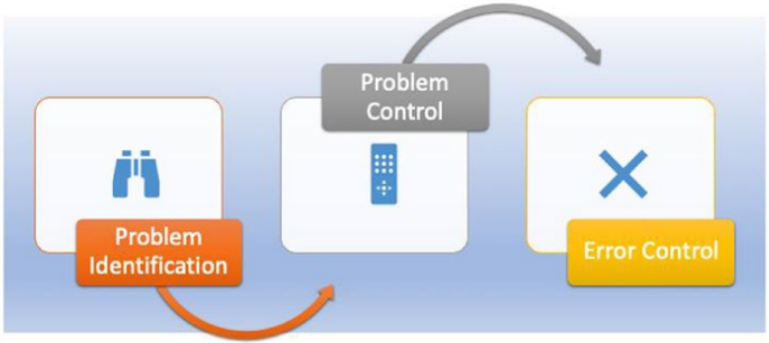
Problem Management Phases

PRADITA University

- Problem Identification: Finding the problem
- Problem Control: Analyzing and prioritizing problems
- Error Control: Implementing permanent solutions
- Techniques: Brainstorming, Five-Why, Ishikawa Diagram

Problem management phases

PRADITA University



Multiple Choice Question

PRADITA University

Which of the following is the correct event definition?

A. Any change of state that is significant for a service or product or related CI
B. Any change of state that triggers changes to the other operational processes
C. Any change of state for CIs that correlates risks and issues to the service and service management processes
D. Any change of state that has significance for the management of a service or other CI