MTAT.08.021
Systems Administration

L12: Incident, Problem Management, Service Desk, Standards and best Practices

Lecture
2011-05-19
Incident Management
(*Intsidendihaldus*)

incident – an unplanned interruption to a service or reduction in the quality of service
Incident Management

Objective of the Incident Management process is to recover from the incidents and return to normal service as quickly as possible
Incident Life Cycle

- detect
- register & classify
- initial support
- possible escalation
- investigate, diagnose
- repair, recover, restore
- close
Problem Management

Incident Management

Change Management

Ulrich Norbisrath (http://ulno.net)
University of Tartu

Systems Administration
http://sysadmin.ulno.net

source: itSMF 2011-05-19
Detecting the Incident

- event from monitoring system
- user reports to service desk
- incidents discovered by IT staff
Classifying the Incident

are we dealing with an actual incident?
  • false alarm
  • no need to take action

incident type
  • fault
  • service request
  • need for assistance
Classifying the Incident

incident category
● hardware, software, network, people, process, documentation...

incident sub-category
● specific to your system
  - hardware – workstations, servers
  - software – operating system, application
Classifying the Incident

components affected by the incident

- service...
- ...or a physical component (configuration item)
- user :)

incident symptoms as described by users

- should not be basis for diagnosis
Initial Support

- recurring incidents
- obvious problems
- simple assistance
- incident-specific workflows

- complicated incident, need for more technical assistance – escalate to next tier of support
Initial Support

recurring incidents

- is there an existing solution (workaround)?
- it is a recurring incident for you, but not always for the end user
- recurring incident is a potential problem
Investigation & Diagnosis

first time incidents

● first, check component status
  - monitoring, events, logs
  - test scripts

● only then, try to reproduce user's problem
  - steps to reproduce
  - is reproducible?
Investigation & Diagnosis

abnormal component status
• consult documentation for maintenance tasks
• replace, restart

reproducible problem
• perform real-time monitoring

no apparent cause – escalate to problem management
Resolution

- assist the user
- apply workaround
- perform maintenance tasks
- request change
Service Desk

Central point of contact between IT and users

• incident management
  - including user assistance
• communication
• educating the users
  - by providing help documentation
Incident Prevention

first contact with Service Desk is usually made only when there are some issues using the system

• ideally, a steady, trusted communication channel to users should be established
  – help documentation
  – information about oncoming changes
End User Assistance

difficulty using the system
  - user is new to the system
  - rarely used function
  - badly designed system

service desk provides (real-time) assistance
pre-compiled help documentation can be used
Communicating

• sensitive and critical changes
• sensitive and critical maintenance
• added functionality, new systems

• multiple sysadmin teams, same communication channel
  – same format

... + improved awareness in service desk
Communicating

from users
  - incident reports
  - service requests
  - feedback

system administrators
  - workarounds,
  - change and maintenance announcements
  - detail inquiries
Documenting

- logging/documenting of incidents is essential
- helps with recurring incidents
- helps new service desk workers to “catch up”
- incident records are needed for incident and problem managers
- user self-training tutorials
- internal training
Types of End User Support

phone and instant messaging

- one of the most expensive methods
- mostly for incident registration and initial support
- possibility to redirect
- number of users simultaneously served is limited
Types of End User Support

self-service ticket systems

• interface to self-register incidents
  – lower classification quality
  – must re-classify?
  – register through service desk, monitor the progress through ticket system

• high number of users simultaneously served

• incident management
Types of End User Support

- local support persons (per organizational unit)
- system-specific support persons
- direct support from system administrators
  - for specific, complex incidents and problems
- provider/vendor support
Types of End User Support

electronic tutorials
• easy to change
• relatively cheap to maintain
• may not be accessible during the incident

printed tutorials
• easy to read due to higher resolution
• usable without a working computer
• costly to produce, hard to change
System Administrators and Service Desk

- “support for user support”
- participating in writing the tutorials
- providing the input for user-IT communication
- direct support in the case of complex incidents
- service desk can be viewed as a monitoring resource
Tools for Service Desk

- incident (ticket) management systems
- remote assistance tools
- monitoring systems
- configuration management systems
Problem Management
(*Probleemihaldus*)

problem is an unknown cause of an incident
Problem Management

the main responsibility of Problem Management is to find root causes of incidents. The objective is to prevent future incidents from happening and to reduce the impact of future incidents
Incident, Problem, Known Error

Incident, Recurring Incident, Potential Incident

Problem Management

Problem (Probleem)
unknown cause of the incidents

Known Error (Viga)
known cause of the incidents

Workaround
(Ajutine lahendus)

Change Proposal

University of Tartu

Systems Administration
http://sysadmin.ulno.net

2011-05-19
29/61
Incident Management

- Incidents
- Incident DB

Problem Management

- Problem DB
- Known Error DB
- Known Errors
- Problems
- Analysis & Diagnosis
- Solution, Change Proposal
- Workarounds

Change Management

- Changes

Ulrich Norbisrath (http://ulno.net)
University of Tartu
Systems Administration
http://sysadmin.ulno.net

Source: itSMF
Problem Management

formal or creative process?

• one of the most complicated processes
• critical for providing a good service
• experience required
• suitable mindset required
incident, problem, known error DB

collect and elaborate on info

problem

monitoring & docs

workaround solution

specific tests

diagnosis, finding the root cause

providing solutions

known error

change proposal

new database records

NOT OK

testing the solutions

OK
From Incident to Problem

• recurring or high-impact incident is escalated

• incident investigation data is forwarded
  – classification
  – ability to reproduce
  – monitoring data, component status
  – which components are affected
  – which users are affected

• overall system status
Detailed Investigation

• check the failing components
• check all the dependencies
• check the logs
  – change debug/log levels
• simulate in test system

• syscall/library call trace (kooodijälitamine)
• network sniffing (võrgu pealtkuulamine)
• memory/data (andmetõmmised)
Finding the Root Cause

- **common denominator** of various symptoms

- **eliminating possible causes**...
  - ...using logs
  - ...detail observations and tests
  - ...considering the area of impact
Finding the Root Cause

- connection to any recent changes?
  - review all the recent changes?
- are there any external influences?

- use your experience
- 😊 fantasize
- 😊 perform a ritual (rain dance, sacrifice) 😊
Providing the Solution

- standard solutions (documented by provider)
- solutions based on other people's experience
  - may not be a good solution
  - may not apply on our case
- temporary workarounds

- final solution – a (formal) change to system
Applying the Solution

- critical, because it affects the system
- think before doing (damage)
- all the steps of the solution must be justified and backed by clear evidence
- use the change management process
Testing the Solution

• are the symptoms gone?
• user feedback
• monitoring feedback
• compare data from real-time monitoring
Problem Solving: Mindsets

- different stages need different mindsets
  - bold, creative
  - critical, strategic

- switching between the mindsets is an art on its own
Problem Solving using Web Search

GIYF!

- how would someone describe such problem?
- searching by the error message
  - same error message may have different root causes
  - most useful when error messages are in English
  - specific error messages will find you nothing
- start with generic search, then specify
Standards and Best Practices

sets of best practices (*parimad praktikad*)
- COBIT (Control Objectives for Information and related Technology)
- ITIL (IT Infrastructure Library)

frameworks (*raamistikud*)
- MOF (Microsoft Operations Framework)
- HP ITSM Reference Model

standards
- ISO/IEC 20000
- ISO/IEC 17799 (27000)
Plan, Do, Check, Act (PDCA)

William Edwards Deming

Act
Plan

Check
Do
Plan, Do, Check, Act

Plan
- set the goals and the steps to achieve them

Do
- execute the plan

Check (Study)
- observe the process, measure results

Act
- analyze the differences between goals set and the actual results, make changes to plan
COBIT - Control Objectives for Information and related Technology

- 1992, ISACA (Information Systems Audit and Control Association)
- aimed to IT executives and auditors
COBIT – coverage

- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate
COBIT package

- Executive Summary
- Governance and Control Framework (34 processes / high level control objectives)
- Control Objectives (210 specific control objectives)
- Management Guidelines
- Implementation Guide
- IT Assurance Guide
Cobit - Overview

IT Governance
- Business and Governance Requirements
- Enabling Information and Technology
- Delivering IT Processes

Plan and Organise
- Direct
- Control

Acquire and Implement
- Metrics

Monitor and Evaluate
- Goals
- Strategic Alignment
- IT Resources: Applications, Information, Infrastructure, People
- Information Criteria and Application Controls
- Process Controls and Process Maturity
- Performance Measurement
- Value Delivery, Risk Management, Resource Management

Deliver and Support

Ulrich Norbisrath (http://ulno.net)
University of Tartu

Systems Administration
http://sysadmin.ulno.net

2011-05-19
48/61
ITIL - IT Infrastructure Library

set of best practices
first created at 1980's by UK government agency

- CCTA – Central Computer and Telecommunications Agency
- now OGC – Office of Government Commerce

divided into processes

- procedures
- roles
ITIL – IT Infrastructure Library

• most popular set of best practices amongst IT service providers today
• current version is v3
• several frameworks are based on ITIL
• set of best practices – does not provide 1:1 processes
  – nor does it have to be followed to the letter
• oht rakendada vormiliselt, mitte sisuliselt
ITIL – IT Infrastructure Library

- Service Strategy
  - Strategy Generation
  - Financial Management
  - Service Portfolio Management
  - Demand Management
ITIL – IT Infrastructure Library

• Service Design
  - Service Catalogue Management
  - Service Level Management
  - Capacity Management
  - Availability Management
  - IT Service Continuity Management
  - Information Security Management
  - Supplier Management
ITIL – IT Infrastructure Library

• Service Transition
  - Change Management
  - Service Asset and Configuration Management
  - Knowledge Management
  - Transition Planning and Support
  - Release and Deployment Management
  - Service Validation and Testing
ITIL – IT infrastructure Library

• Service Operation
  - Event Management Process
  - Incident Management Process
  - Request Fulfillment Process
  - Access Management Process
  - Problem Management Process
  - Service Desk Function
  - Technical Management Function
  - Application Management Function
  - IT Operations Management Function
ITIL – IT Infrastructure Library

• Continual Service Improvement
  – 7-Step Improvement Process
  – Service Measurement
  – Service Reporting
ITIL – IT Infrastructure Library
Microsoft Operations Framework

- Business/IT Alignment
- Reliability
- Policy
- Financial Management

- Portfolio
- Operational Health
- Service Alignment

- Envision
- Project Planning

- Build
- Stabilize
- Deploy

- Governance, Risk, and Compliance
- Change and Configuration

- Release Readiness
- Team

- Operations
- Service Monitoring and Control
- Customer Service
- Problem Management

Ulrich Norbisrath (http://ulno.net)
University of Tartu

Systems Administration
http://sysadmin.ulno.net

2011-05-19
57/61
HP ITSM Reference model

based on ITIL

• Business-IT Alignment
• Service Design and Management
• Service Development and Deployment
• Service Operations
• Service Delivery Assurance
ISO/IEC 20000

first standard for IT Service Management

contents:

- Scope
- Terms & Definitions
- Planning and Implementing Service Management
- Requirements for a Management System
- Planning & Implementing New or Changed Services
- Service Delivery Process
- Relationship Processes
- Control Processes
- Resolution Processes
- Release Process
ISO/IEC 27002

- Information technology - Security techniques - Code of practice for information security management
- Information security standard
- Renamed from ISO/IEC 17799:2005 at 2007
- In Estonia: EVS-ISO/IEC 17799:2003
UT Sysadmin

• Write down two points each
  - What was good in the course?
  - What was bad in the course?
  - What could be better, what would you have liked to see?
• Discuss with 1-2 neighbors, compile down to one list with two each.
• Report (and publish on discussion board).