A Case Study on Improvement of IT Service Incident Investigation Process

Kari Saarelainen, KPMG Finland
Marko Jäntti, University of Eastern Finland

22nd EuroAsiaSPI Conference
Ankara, Turkey, 30.09.-02.10.2015
Content

Swiss Cheese and HFACS
Big picture - Core processes in ITSM
The idea of latent factors in incidents
Research methods
Root causes of incidents in this case
Incident investigation process
Incident trend analysis
Improvement opportunities
Lessons learnt
Where we come

University of Eastern Finland, Kuopio

KPMG Finland, Helsinki
Why to study IT incidents

IT services are everywhere in our life.

If IT fails (=incident), one cannot e.g.

- Pay with credit cards
- Sell or buy stocks
- Buy train, plane, concert, etc. etc. etc. tickets
- Make fixed and/or mobile calls
- Make and send radio, TV programs and newspapers
- Send and transfer postal packets
- Operate a paper mill
- Feed and milk cows

How to ensure, that IT runs constantly

- Fault tolerant design, no single points of failures
- Profound training to experts
- Standard operating processes

Still incidents happen

This study presents one method to improve the quality of IT service
Big picture: IT Service Management (ITSM) and the scope of this work

IT Service Management (ITSM)
– The implementation and management of quality IT services that meet the needs of the business. IT service management is performed by IT service providers through an appropriate mix of people, process and information technology.

IT Infrastructure Library (ITIL) / ISO 20000
– De-facto standards in ITSM
– Examples of ITIL processes: Request fulfillment, change management, incident management, problem management, etc.

Incident management process
– Tries to return the IT service to customers as quickly as possible.

Problem management process
– Tries to find the root cause of a single incident or recurring incidents
HFACS taxonomy in root cause categorization - Swiss Cheese Model (SCM)

Swiss Cheese model of incidents

- By James Reason 1992
- Concept of active and latent failures in human error related accidents and incidents
Human Factors Analysis and Classification System (HFACS)

**HFACS levels**
- Unsafe Acts
- Preconditions for Unsafe Acts
- Unsafe supervision
- Organizational influences

**HFACS categories**
- The actual root cause categories

---

© 2015 KPMG Oy Ab, a Finnish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.
The idea behind HFACS and Swiss cheese applied in IT

Not any more “human error” or “configuration error” as a root cause

Seek the contributing factors, latent causes behind this, e.g.

- Poor change plan
- Poor test plan
- Preparing these plans not supervised
- Implementation was done against the process/instructions
- Compliance to process is not supervised
- Poor training for experts
- Process does not require testing
- Lack of monitoring/trouble shooting tools

Fix these, so the actual harmful acts will be fixed

But does this work in practice?
Research Questions

RQ1: What is the role of incident investigation in continual service improvement cycle?

RQ2: Is HFACS taxonomy suitable in categorization of ITSM incident related to human factors?

RQ3: How is categorization of ITSM done during the incident investigation and after incident investigation as part of incident trending?
Methods: Data Collection and analysis

**Action research (Baskerville)**

**Data collection**

**Multiple data collection method**
- **Documents**
  - Incident reports
- **Meetings and discussion with managers**
  - Interviews with managers and supervisors
  - Interviews experts involved in the incident
- **Records and archives**
  - Change, incident and problem records.

**Data Analysis**
- Within case analysis
- Validation in workshops
About incidents

**Official definition:**
An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident – for example, failure of one disk from a mirror set.

**From small to major incidents**
- Small: printer is out of paper
- Major: the bank system is down

**Life of an incident**
- Identification (human or machine)
- Logging, categorization, prioritization
- Resolution
- For medium of larger incidents: Root cause analysis
- Incident trend analysis for service improvement
Root causes and their occurrences

72 incident reports with human errors

Observations

Not enough info in the reports
- > 50% of reports did not have enough information to fit in any HFACS category.
- E.g. configuration error
  - The most common error type
  - Error: Skill-based, decision, perception
  - Violation: Routine, exceptional

HFACS not always IT oriented
- Perception error
- Skill based vs. decision based
- E.g crew resource management vs. team work

Reports not HFACS compliant
- See next page

<table>
<thead>
<tr>
<th>Generalized root cause</th>
<th>Occurrences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect configuration/parameter/command</td>
<td>32 %</td>
</tr>
<tr>
<td>Communication problem</td>
<td>8 %</td>
</tr>
<tr>
<td>Inadequate testing</td>
<td>8 %</td>
</tr>
<tr>
<td>Omitted instructions</td>
<td>8 %</td>
</tr>
<tr>
<td>Poor process design</td>
<td>6 %</td>
</tr>
<tr>
<td>Wrong port/tube/fiber/device/connector</td>
<td>6 %</td>
</tr>
<tr>
<td>Required service/feature was not activated</td>
<td>5 %</td>
</tr>
<tr>
<td>Fail to estimate consequences</td>
<td>3 %</td>
</tr>
<tr>
<td>Inadequate plan</td>
<td>3 %</td>
</tr>
<tr>
<td>Inadequate supervision</td>
<td>3 %</td>
</tr>
<tr>
<td>Violation of process</td>
<td>3 %</td>
</tr>
<tr>
<td>Error in instructions/documentation</td>
<td>2 %</td>
</tr>
<tr>
<td>Poor system design</td>
<td>2 %</td>
</tr>
<tr>
<td>Cooling was deactivated by accident</td>
<td>2 %</td>
</tr>
<tr>
<td>Other root causes</td>
<td>7 %</td>
</tr>
</tbody>
</table>
Model of accident investigation

I. Collecting data
II. Hypotheses generation
III. Analysis
IV. Findings
V. Recommendations

Root cause analysis (RCA)

Iterative process

By European Safety Reliability and Data Association (ESReDA)
Incident trend analysis

If the incident analysis framework (here HFACS) is not applied already in the original incident investigation, the result is very unsatisfactory.
Incident investigation and trending are part of continual service improvement

1. Identify the strategy for improvement
2. Define what you will measure
3. Gather the data
4. Process the data
5. Analyse the information and data
6. Present and use the information
7. Implement improvement

- Plan
  - Initial, a priori knowledge, model, e.g. HFACS
  - Collecting data
  - Hypotheses generation

- Do
  - Analyses

- Check
  - Findings
  - Recommendations
Summary: Lessons learnt

Lesson 1
– Seek contributing factors beyond “configuration error”

Lesson 2
– HFACS needs adaptation to ICT

Lesson 3
– Use HFACS already in the incident investigation

Lesson 4
– Take incident investigation and incident trending as a part of continual service improvement
Any questions?