DITY™ Weekly Newsletter
itSM Solutions®
IT Experience. Practical Solutions
The workable, practical guide to Do IT Yourself
Vol. 6.8 • February 26, 2010

9 Steps to Better Incident Classification

By Hank Marquis
Hank is EVP of Knowledge Management at Universal Solutions Group, and Founder and Director of NABSM.ORG. Contact Hank by email at hank.marquis@usgct.com. View Hank's blog at www.hankmarquis.info.

Incident classification is one of the most important and most difficult aspects of ITIL to implement. The benefits far outweigh the managerial challenges involved.

Through Incident Classification and Initial Support, Service Desk staff aims to determine the reason for an Incident, and how to route it for resolution.

The IT Infrastructure Library (ITIL®) spends considerable time discussing classification. There are many free forms and checklists available, and most automated systems offer built-in assistance with classification.

Yet many IT organizations struggle with classification, and "unknown" or "other" is often the most common classification -- indicating the classification process has failed.

Such Incidents tend to bounce from group to group and suffer many escalations and transfers. These "bouncing" Incidents consume significant organizational resources and inflict poor service on Users and Customers.

Luckily, there are several quick-and-easy fixes for this problem. Following I describe 9 simple steps to improving Incident Classification and offer a simple classification scheme.

About Classification

All classification boils down to trying to understand and identify what systems are impacted and to what degree. In this article, I focus on classification and leave the topic of assigning a priority to a later date.

Effective Incident classification aids in routing the Incident to the correct team on the first try. Why is classification often done incorrectly, even with all the resources, tools and time dedicated to the subject?

Incident classification starts to go wrong when diagnostic scripts (scripts) become too complex. While extremely valuable, scripts require diligent management effort. However, trying to collect massive amounts of data through dozens of questions slows the process down, complicates the workflow, and results in incomplete classification. A simple observation is to keep your diagnostic scripts as simple and purposeful as possible.

Checklist for Improving Incident Classification

To simply the classification process, improve its efficiency and begin to reign in those "unknown bouncing Incident" consider the following:

- **Use Diagnostic Scripts** – Use scripts to standardize and formalize Incident Classification. Without sound scripting procedures (manual or automated), you cannot develop the management information required to ensure their effectiveness. Without a repeatable process (e.g., a script), you cannot reliably classify Incidents.
- **Classify by CI, Not Symptom** – Be sure that you are not using documented symptoms as your classification. Symptoms change and can be misleading. Document the Configuration Item (CI) judged to be at issue. Record the symptoms in a comments field, but know that different Users will report different symptoms for the same Incident. Classifying on symptom is worst practice!
- **Classify Incidents, Not Calls** – Be sure that you are actually performing Incident Classification, not simply logging calls. If you are logging calls, then do not bother trying to perform Incident Classification. Logging calls is a

very different activity from Classification and Initial Support. Call logging simply gathers route data a specialist will use later.

- **Keep it Simple** – Review your diagnostic scripts often, make sure they do not get so complicated that staff cannot complete them in a reasonable amount of time. Include as a diagnostic code "other" or "unknown" and track these codes. Such codes are an indicator that your scripts need maintenance.
- **Use Your Service Catalog** – If you have a Service Catalog, use it. If you do not have one, consider implementing one. Referring to a service in a catalog speeds the Incident logging activity. It also results in less information collected and thus less paperwork. Finally, it provides an increase in the accuracy of data in the Incident record and can assist in routing, escalation, and support.
- **Leverage Your Tools** – Many of the automated tools available today provide sound support for Incident classification. Investigate the capabilities of whatever system you have. If appropriate, use these features. Just remember to keep the rules as simple as possible.
- **Assess Your Maturity** – Honestly asses the maturity of your organization, processes and people. A phased approach over time is the best approach in most cases. This is especially true for new or immature organizations. The reason for the assessment is to establish a reasonable expectation of capability and performance before rolling out your new Incident classification system! Highest efficiency only occurs when you have at least basic Configuration, Problem, and Service Level Management in place.
- **Validate Your Scope** – It is very important to realize that not every single event that occurs warrants an Incident. It is easy to set your scope too wide or too narrow. Too wide and every normal automated system event can become an Incident, swamping your staff and systems. Too narrow and you are not delivering the highest value. The rule of thumb is to raise an Incident only if there is some action required. This means that normal diagnostic messages on throughput, utilization and so on should not be incidents. Set your scope carefully for highest performance.

Simple Classification Scheme

Configuration Items (CI) form the basis of all classification. The question is one of depth. Often classification takes one of two tacks:

1. Classifying based on the physical CI (e.g., Workstation, Software application, etc.)
2. Classification based on IT service CI (e.g., Order Entry, Internet, etc.)

At a minimum, your classification should operate on physical CI. As you mature (that is, have more defined Service Level Management) you can expand into affected IT service as well. An effective and simple classification scheme:

1. Type
2. Category
3. Sub-category

The Type field is to concentrate the required support by the kind of Incident. [Often this is where prioritization begins as well.] There are three basic kinds of Service Desk interactions described in the ITIL:

1) Fault/failure, 2) Service Request (ITIL's Request Fulfillment Process), 3) Assistance/Inquiry

The Category field is to select a technology domain of expertise. Try to keep the Category field down to as few major areas as possible. Since we are going to base of system on physical CIs (to start), then a simple list of ITIL CI types like the following is good:

- Hardware, Software, Network, People, Process, Accommodation, Documentation

The Sub-category drives the specific group within the technology expertise domain identified by the Category. Entries here are quite specific to your organization. Here again it is best to keep the list as small as possible while still routing effectively. Some examples here might be

- Hardware: Workstation, printer, monitor, router, PBX, phone, etc.
- Software: Word processing, spreadsheet, database, order entry, etc.
- Accommodation: Move/Add/Change, etc.

The output of such a system might look like this:

- Type: Fault/Failure
- Category: Software
- Sub-category: database
- Note: User reports "SQL error" when looking up customer "J. Jones"

Note how the user reported symptom is included in the notes, but that the diagnosis is based on CI. Such a system is easy to develop, easy to script, and easy to implement. It is also going to be quite effective at routing Incidents properly.

Benefits of Effective Classification

Successful Categorization helps in many ways, here are a few of them:

1. Quickly find solutions (workarounds and/or fixes) to Incidents
2. Properly route Incidents to the correct support group
3. Gather sufficient data to speed diagnoses by nth level support
4. Aids Problem Management in building and maintaining a knowledge base
5. Improves efficiency of technical/functional groups
6. Enhances Customer satisfactions
7. Increases User productivity
8. Builds maturity toward more proactive operations

Summary

Incident classification is one of the most important and most difficult aspects of ITIL to implement. The benefits far outweigh the managerial challenges involved.