itSM Solutions® DITY™ Newsletter Reprint

This is a reprint of an itSM Solutions® DITY™ Newsletter. Our members receive our weekly DITY Newsletter, and have access to practical and often entertaining articles in our archives. DITY is the newsletter for IT professionals who want a workable, practical guide to implementing ITIL best practices -- without the hype.

become a member

(It's Free. Visit http://www.itsmsolutions.com/newsletters/DITY.htm)

Publisher
itSM Solutions™ LLC
31 South Talbert Blvd #295
Lexington, NC 27292
Phone (336) 510-2885
Fax (336) 798-6296

Find us on the web at: http://www.itsmsolutions.com.
To report errors please send a note to the editor, Hank Marquis at hank.marquis@itsmsolutions.com
For information on obtaining copies of this guide contact: sales@itsmsolutions.com

itSM Solutions®
IT Experience. Practical Solutions.

Subscribe PDF Download Back Issues

Vol. 3.1 JANUARY 3, 2006

How To Prioritize Incidents

DITY Weekly Reader

The workable, practical guide to Do IT Yourself

IT should work on those things that are of a critical nature first, not simply those things people want done right away. The cold hard truth is that not every incident can or should be Critical.

hank MARQUIS

Articles
E-mail
Bio

By Hank Marquis

We all know that every customers outages and issues are the #1 AAA top highest most important things in their world, and they expect us within IT to respond appropriately—OR ELSE!

Of course we in IT get lots of these "we need it now" incidents, which most of us refer to as "Urgent" requests. None of us have unlimited resources, so how can you balance response to all these requests for critical assistance?

Clearly, some form of prioritization is required. But many times simply mentioning the word "prioritize" in a meeting brings up bad feelings and posturing on both sides of the table—"us" and "them."

I think part of the problem is using the term "Urgent" to describe a priority. It does not

clearly communicate the nature of the situation. I prefer the term "Critical" to refer to the most important thing IT can do instead. I think this also helps in the conversation with the business.

IT should work on those things that are of a critical nature first, not simply things people want done right away. The cold hard truth is that not every incident can or should be Critical.

We have to establish a prioritization system that works, is fair, and takes into account true business need and IT capability. Oh yes, and one the customer accepts and agrees to follow.

I find it helpful to use non-technical analogies to work with business people, especially when trying to get them to understand something complicated. So, in order to come to a priority system that works, let's start by examining one we all have heard about—the use of "alarms" by your local fire department. You know, a "2 alarm fire" or a "4 alarm fire" and so on.

Once again, real fire fighters provide an excellent model for IT.

How Fire Fighters Do It

A priority code is a value assigned to a work request, like an incident record. The priority code establishes the order in which jobs gets done and ensures the correct allocation of resources required to accomplish the work the job requires in the timeframe permitted. Priority reflects the organizational response required for an Incident. Simply put, an issue with a higher priority gets resolved sooner than a lower issue because we apply more focus and more resource sooner.

Fire departments often have a priority system based on "alarms" to indicate priority. One department uses a scheme that has 5 levels of priority—where priority means level of resource applied to the issue. More urgent needs get more resources sooner in an escalating manner. It begins when an initial call is evaluated, and assuming a credible report of fire; the response is 5 fire engines, 2 ladder trucks, one rescue squad and one fire chief.

- A 1-alarm fire is one confirmed by the initial responders; and one more engine, one more ladder truck, one battalion fire chief and one ambulance are committed to the effort.
- A 2-alarm fire brings 4 more engines, 2 more ladder trucks, 1 more fire chief and EMS equipment.
- A 3-alarm fire gets 4 more engines and 2 more ladder trucks.
- 4-alarms signal a huge fire and the department sends all available equipment and personnel.

Stay with me here! Fire fighting is a pretty well established business, and the schemes used have been proven. They know how and when to respond, and what resources they need to apply. Key points to notice here include:

- The response level (e.g., priority or "alarms") is described in terms of how the support organization responds and not the scope or criticality of the situation
- There are 5 types of response (initial, to 4 alarms), each indicating increased managerial and technical commitment
- For each type of response there is a pre-defined resource allocation and process
- Technical evaluation of the situation determines the response type
- Few situations immediately receive a "4-alarm" response
- Escalation provides more technical and managerial focus and resources

How You Can Do It

Fire fighting is actually a pretty good model for how IT might respond to incidents. It all begins by defining what resources you have available and how you want to deploy them. This requires a framework for evaluation and escalation. I am going to leave the topic of escalation for later, and focus on priority establishment.

It is very important to separate a priority from the establishment of that priority. A priority code, for example *Critical*, defines how the organization will respond. It is separate from the *reasons* an event or incident is handled *Critically*. This is a crucial distinction to understand. Many otherwise well intentioned priority coding system run amuck due to confusing this fact. Practically, this means that establishing a priority coding system requires two major parts:

1. definitions of organizational response (e.g., Critical, High, Medium, Low, etc.)
2. a method for determining which response to apply to any given incident

ITIL presents an example (and it is just an example) of a 2-part priority coding system with five priority levels or tiers: 1-Critical, 2-High 3-Medium, 4-Low and 5-Planning. It then offers a simple matrix with impact on the top, and urgency on the side to select the priority.

Thus, establishing priority is a matter of mostly two things: impact and urgency. Impact is what will happen if the job does not get done and urgency is a measure of how quickly a job has to get done. A third element, resource allocation, can also be used and relates to scope, in other words, how many "fires" you want to be able to fight at once.

Of course, as is most often the case with ITIL, necessarily left completely up to the practitioner is the definition of impact and what constitutes urgency. This makes the next big question "how do impact and urgency get determined?"

Start by defining what a Critical priority (code 1) means in terms of how the IT organization will respond to it. Here is one set of definitions taken in part from an actual organizations stated policies:

> *CRITICAL priority means an immediate and sustained effort using all available resources until resolved. On-call procedures activated, vendor support invoked.*

Note how the priority describes how the IT organization will respond. It is not a description of some customer outage, affected users, or litany of services. Instead, it establishes the basis for servicing the customer. Any reasonable customer would now understand that given such definition of Critical (priority 1) issues, many so-called "urgent" or "critical" requests are not truly urgent or critical after all. How can the IT department apply "all available resources" (internal and external) to every issue? They can't and should not have to either.

The number of priority definitions, and how long it has to respond, should be worked and agreed with the business and take into account any service catalogs and service level agreements.

Next describe the rest of your levels:

> *HIGH priority means technicians respond immediately, assess the situation, may interrupt other staff working low or medium priority jobs for assistance.*
>
> *MEDIUM priority means responding using standard procedures and operating within normal supervisory management structures.*
>
> *LOW priority means responding using standard operating procedures and as time allows.*

After defining the responses, we now have to develop a workable matrix (in conjunction with the business) to choose which response will be used for any given incident. One example considers several impact aspects in addition to urgency, and assigns a numeric point value to a variety of applications, customers, situations, and so on. Figure 1 shows three aspects: Scope (number of affected users), Goodwill (visibility), and Operations (functional interference). Note that the number of impact aspects should be worked and agreed with the

business. Don't have too many impact aspects or scoring an incident becomes troublesome.

In figure 1, each IMPACT and URGENCY column can get earn from 0 to 3 points. For example, an Incident may have a Scope impact of 3, a Goodwill impact of 0, an Operations impact of 1, and an urgency of 2, and thus score a 6:

	IMPACT	IMPACT	IMPACT	
Points	Scope	Goodwill	Operations	URGENCY
3 points each	Affects > 50% of users	Areas outside of the company will be affected negatively OR positively	Interferes with core business functions OR loss or potential loss of mission critical data	Event underway and it cannot be stopped or changed AND immediate action could resolve the issue
2 points each	Affects >10 but < 50 users OR no more than 50% of all users	The company will be affected negatively OR positively	Interferes with non-core activities OR functions that do not affect the entire company	Event scheduled to occur but enough time remains to respond without impacting event
1 point each	Affects < 10 users OR no more than 25% of all users	Business unit will be affected negatively OR positively	Interferes with normal completion of work OR tasks are more difficult but not impossible to complete	Event can be postponed OR is far enough away in time to allow response without loss of productivity
0 points each	Affects a single user	Goodwill unchanged	Interferes with recreational OR non-business related use	No scheduled completion time is required and normal work can continue until responding

Figure 1. Priority Scoring Matrix

We then go back to the priority codes (Critical, High, Medium, Low) and establish a value range for each. In this case a score of 12 means Critical; 9-11 means High; 5-8 means Medium; and 0-4 means Low. You will also need to establish the timeframes within which each priority code will occur. Such a matrix would look like figure 2. Following our example with a score of 6, this incident would be receive a priority of Medium:

Score	Priority Code	Response	Timeframes
12	Critical	An immediate and sustained effort using all available resources until resolved. On-call procedures activated, vendor support invoked.	Immediate action/resolution as soon as possible.
9-11	High	Technicians respond immediately, assess the situation, may interrupt other staff working low or medium priority jobs for assistance.	Action within 1 hour/resolution within 1 business day.
5-8	Medium	Respond using standard procedures and operating within normal supervisory management structures.	Action within 2 hours/resolution within 2 business days.
0-4	Low	Respond using standard operating procedures as time allows.	Action within 2 business days/ resolution within 10 business days.

Figure 2. Priority Assignment Matrix

To use the system, the agent will simply score the incident by adding up the conditions met in figure 1 to come to a total, and then choosing the appropriate priority code from figure 2!

Summary

Incident priority defines how the organization will respond. It takes into account multiple aspects of impact (e. g., scope, application, service, reputation, environment, business, etc.) and urgency (e.g., how much time IT

has to get the job done.)

1. Define your priority codes working with the business and as many unique Customers or representatives of departments or business units as possible. (They will soon realize that not everything can be Critical!)
2. Agree to definitions of what resources you will bring to bear (e.g., how you will respond) BEFORE you agree timeframes.
3. Agree to timeframes BEFORE you attempt to determine the business impact/urgency matrix.
4. Select, define and agree the impact columns, and an urgency column.
5. Develop, agree, and share your incident priority system with the business.
6. Train service desk staff, and then deploy. (Be sure to provide copies to customers and users so that they understand how decisions on priority will be made from now on.)

A sound prioritization scheme like the one presented here can help you stabilize your day to day operations, make you less reactive and more even in your responses. It improves reporting, and since you developed it in conjunction with the business it lets you align more closely with customers and users, bridging the "IT Business chasm."

You might even find that in time, you get less and less of the "we need it now" from customers. We in IT can all learn something from people who really fight fires!

--

Where to go from here:

- Subscribe to our newsletter and get new skills delivered right to your Inbox, click here.
- Download this article in PDF format for use at your own convenience, click here.
- Browse back-issues of the DITY Newsletter, click here.

Related articles:

- How to Classify Incidents explains how to establish Incident classification systems.
- 9 Steps to Better Incident Classification explains Incident classification.
- Scripted Success for more on creating and using diagnostic scripts.