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

DITY™ Newsletter
Vol. 3.3 • January 17, 2007

Impact Assessment In 5 Simple Steps

Subscribe Its Free! RSS Stay up to date! PDF Pass it around! Print page

IT is its own worst enemy—Gartner and others have documented that about 80% of all Incidents occur because of failed change management activities. However, it does not have to be that way. Change Impact Assessment is well known outside of IT...

By Hank Marquis

Anyone familiar with ITIL® has heard of an “Impact Assessment.” While there are many places in the ITIL that mention assessing impact, this article focuses on assessing the potential impact of changes. Change impact assessment is a systematic approach that seeks to discover possible risks associated with a Request for Change (RFC.)

Failure to discover the risks of a proposed change is the top reason for that popular dance, the IT 2-step. Everybody knows it, it goes like this "take one step forward, now two steps back..." Seriously though, most failed changes are simply the result of not taking into account current activities, and a failure to communicate anticipated activities.

This includes any situation which proposes to alter system configurations, operating practices,

policies, or procedures, and any new or different activities to be performed.
For change impact assessment, or simply impact assessment, to be effective the practitioner has to explore all of the differences between normal operations and any conditions that introduce risks or may contribute to a failed change.
Used effectively, impact assessment can proactively manage risk. It is a simple idea that can be implemented quickly using a word processor or spreadsheet -- it requires no complex software. It does require careful adherence to a formal procedure however, and teamwork.
Following I describe how to reduce the risks of making changes by introducing a simple, effective, formal change impact assessment procedure based on best practices.

Impact Assessment 101

Impact assessment is a fairly mature and formal activity in most organizations outside of IT, the military in particular has deep experience in planning changes. Yet for some reason most IT impact assessment consists of emailing around an RFC and waiting for someone to comment about it, or worse, a lead tech working in isolation on "one little change." Another popular method I see for impact assessment is a meeting, usually the day or two before the change is to occur, where department heads talk about the work upcoming.
However, it is clear that existing impact assessment does not work. Every year all the big think tanks always report that IT is its own worst enemy—Gartner and others have documented that about 80% of all Incidents occur because of failed change management activities. However, it does not have to be that way. Change impact assessment is well known outside of IT, and there are models for performing impact assessment.
While effective and easily implemented, impact assessment is not a panacea and does not totally replace existing change procedures, instead, you should strive to improve your existing process. The procedure for performing an impact assessment consists of the following five steps:

1. Define the extent of the change proposed
2. Determine key differences in the changed state (proposed) from a point of reference or the original state
3. Focus on the possible effects of the key differences from step #2
4. Sort and prioritize the possible effects (#3) from the key differences (#2) based on risk and possibility
5. Make a decision using the results

Sounds easy! So lets actually try to use our new system.

Step #1 -- Define Extent of the Change

Assuming you have in hand an RFC that wants to "Upgrade Desktops to Vista", prepare a document (word processor is fine) that describes the extent of the change. Be specific, and list all boundaries for all systems. Without a clear understanding of the change, you can't identify risks. Clearly, some of this will be in the RFC already, but you need to make sure to capture all possible descriptions of the environment for the change.
Take a tact of tying to identify what will probably occur or be going on before, during, and after the change. Try to consider as many environments or angles as possible. For example:

Probable Events With "Upgrade Desktops to Vista"

- Scope: Initial upgrade IT department only, IT non-production workstations only, no servers, no desktops, laptops only.
- Work Environment
  - Some IT workers only have laptops
  - Some workers will be traveling and not in the office
- Platform Environment
  - Disk space requires is 300MB
  - Transition of existing preferences, installations, and configurations
  - Memory required is 2GB
  - CPU speed must be at least 1.2GHZ

Table 1. Probable Events

Your goal here is to describe, as fully as possible, the environment and situation for the change. The more detail, the better.

Step #2 -- Determine Key Differences

The basis of the impact assessment is to compare the proposed state of the infrastructure or organization after the change with the state before the change. Of course, with something new there is no existing baseline, in which case you can choose a similar situation, or even do research about other implementations.

The goal is to identify all of the differences, large and small, between the pre and post -change states. Examine previous changes. Check for similar changes in other systems, departments, technology silos and divisions. Check for failures by reviewing past change records, incident logs, and problem reports. Review the Internet for documents describing what others have found and done.

After establishing your reference sources, in a table list out all the differences between the references (failures and success.) Don't try to sort, categorize, or judge them. Your goal is as many types of differences as possible. Common differences include:

- Hardware and software models, versions, platforms, etc.
- Staff, personnel, vendor, and support persons, etc.
- Process, procedures, organization, schedules, time of day, etc.
- Environment, location, installation, etc.

This step is ideal for use with a group—assemble a team, give them the reference data in advance, have them prepare, then host a meeting where you can lead a brainstorming session to develop as many potential differences as possible. Record them into a table, with references, for use in the next step. Assuming the previous probable events table (like table 1), a possible output (for example purposes only) might look like this:

Key Differences Between Normal and "Upgrade Desktops to Vista"

- Work Environment/ Some IT workers only have laptops
  - they will be working using their laptops (not available to upgrade)
  - might not be in office at the appropriate time (e.g., work/travel)
- Platform Environment/ Disk space requires is 300MB
  - Previous changes needed less disk space (was 512MB)
  - Several changes backed out due to lack of disk space (had 1GB)

Table 2. Key Differences

Here it is very important to uncover positive, negative, and neutral trends. This means you should check

for successful changes as well. Don't forget to consider your regulatory environment, and you can also use theoretical models like the ITIL and others, that describe a “perfect world” and compare the change to it.

Step #3 -- Focus on Effects

Study each of the differences listed in the table created in the last step (table 2). Ask if this difference has the potential to cause unexpected side effects. Consider the reference materials—has their been a history of fault or failure because of this difference? Has this difference not had any impact? Be sure to imagine positive, negative and neutral affects. This step is also ideal for a group.

Impact Assessment of Upgrade Desktops to Vista			
Differences from Normal	**Potential Effects**	**Risk Mitigation**	
		Prevention Steps	**Monitoring Steps**
Some IT workers only have laptops	They might not be in the office	Ensure accurate listing of all laptops and workers	Step up inquires about which applications are required
	They will have work to do	Make sure there is a system available to users during the upgrade	Step up inquires about which applications are required

Table 3. Possible Effects of Key Differences

Your goal here is to consider the differences for each probable event. For each potential effect, try to list out what you can do to detect it (monitor) and prevent it. This forms the basis of the impact assessment, for the starting point for risk assessment.

Step #4 -- Sort and Prioritize

Using the risk analysis system I presented in “10 Steps to Do It Yourself CRAMM”, make an effort to prioritize potential effect; taking into account the effort, costs, and probability of its occurrence. Of course, full probability assessment is beyond the scope of this article, but you can get pretty close.
Your output is a list of recommendations, with pros and cons, to submit to the CAB or whomever requires it. Your work is self-justifying. That is, using plain simple terms, past experience, and formal planning, you will present what is currently happening, what might happen and ways to make sure the bad does not occur. This is all it takes for leaders to make decisions and prepare.

Step #5 -- Make a Decision

Use the results of the sorted, prioritized risk assessment to identify vulnerabilities and make recommendations to mitigate the risks. Use the recommendations to show how to avoid, or if too costly, respond effectively, should something go wrong with the change. Compare the benefits of following your recommendations to the potential costs of not following them. Decide whether the potential risk is acceptable or not.

Summary

A formalized approach to change impact assessment is inexpensive and can produce high quality decisions. It requires following a process, and having the time to follow a process. While the approach presented here is well tested and sound, it does have some limitations:

- This method relies heavily on the references you choose -- choose the wrong reference or miss a reference and it might not work as well
- Without a CMDB that incorporates organizational learning it is hard to find references
- Your results will only be as good as the knowledge and skills of the people performing the assessment

Even with these caveats, this is still probably the easiest and simplest method to formalize change impact analysis. Follow these simple steps, and you just might find yourself out of the "one step forward, two steps back" routine!

 Subscribe Its Free!  RSS Stay up to date!  PDF Pass it around!

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.
- Use your favorite RSS reader to stay up to date, click here.

Related articles:

- 10 Steps to Do It Yourself CRAMM explains how to establish a risk assessment system.
- Browse back-issues of the DITY Newsletter, click here.