IT RISK ASSESSMENT AND ITSM SERVICE DELIVERY: WHAT YOU NEED TO KNOW

When planning a Data Center change such as deploying a new server or adding a new telecommunications line, mobile application, or Web-based service, it's important to understand the risks and consequences that can occur after your project is deployed. Today, let's look at the role that risk assessment plays when planning a Data Center change in an IT Service Management (ITSM) environment, and how a formal risk assessment approach helps you identify, evaluate, and respond to the risks associated with any new change.

Why use risk assessment?

There is no change without risk. A risk is simply something that introduces uncertainty into the process so that you may not get the outcome you're looking for. Whenever you change or add a service in a corporate or cloud Data Center, some risk is added to the system.

Risk assessment and planning allow you to identify potential risks in new and changed Data Center services and determine how the system will respond to each risk, if it occurs.

Risk assessment and planning belong in the *Service Design* phase of the ITIL Service Lifecycle, where each potential risk can be identified and planned for. Risks can generally be responded to in the following ways and these responses will inform and affect your new service design and may change management planning.

- *Avoidance* – You don't implement any part of the service that could trigger the specific risk. You avoid the risk by not implementing the proposed change.
- *Contingency* – A response is executed after the risk starts to occur. The system looks for a warning sign (trigger) that the risk is happening, and executes a "Plan B" to deal with the risk as its occurring.
- *Mitigation (Reduction)* – You take action in advance to reduce the probability of a risk occurring. The risk hasn't occurred yet but your risk mitigation planning makes it less likely to occur.
- *Retention* – There is no planning in response to a possible risk. You implement the change, accept that the risk and its accompanying losses can occur, and handle the situation after the fact.

From impact to response

When performing risk assessment for a new service, it's important to look at how likely it is that the risk will occur (its *probability*) and how much damage the risk can incur when it happens (its *risk level* or *impact*).

There are many different ways you can determine and rank the probability and impact of each risk. Risks are generally ranked from highest impact/highest probability down to lowest impact/lowest probability with the higher ranked risks demanding more attention during implementation.

Risk rankings can have a significant effect on service design, affecting several items in your delivery process, including:

- If the risk is severe enough, whether your organization may cancel the project altogether (avoidance response)
- Which risks need contingency plans (Plan B), when certain risks manifest themselves (contingency response)
- Which risks require service delivery modification to reduce the probability of the risk occurring (mitigation response)
- Which risks can be ignored because their probability of happening is too low or their impact is minimal to the service or equipment being delivered (retention response)

Some software packages such as BMC Remedy, include automated risk assessment questionnaires for this purpose. Once filled out, the Remedy system uses the questionnaires to determine risk levels and creates a *Change Risk Report* that can help determine the next actions on a change.

The key to risk assessment is that once you understand the most important risks involved with each change and the probability and impact each risk carries with it, you can determine which responses (avoidance, contingency, mitigation, and retention) should be employed to successfully implement the new change.

Risk assessment and Data Center projects

For Data Center changes, we can generally classify most IT changes as belonging to one of two categories.

- Equipment changes – Servers, switches, firewalls, routers, wireless access points, UPS systems, Web filters, phone systems, generators, etc.

- Outside Service changes – Telecom lines, telephone lines, Internet service providers, email providers, Web services, mobile applications, etc.

Within these general categories of equipment changes and outside service changes, we can create a table showing the specific risk categories associated with Data Center changes.

Specific risk categories for Data Center changes

Configuration mistake
Cyber attack
Defective equipment
Equipment failure
Human error
Legal or business issue resulting in loss of service
Natural disaster (flood, earthquake, tornado/hurricane, fire, etc.)
Power issue (inside organization)
Power issue (outside organization)
Replaceable component fails (batteries, hard drives, fans, filters, etc.)
Service interruption caused by vendor or business partner failure

These risk categories define the general risks associated with Data Center projects. Most organizations should be able to identify their own specific risks within each category and be able to rank each risk for its probability, impact, and responses. You should also consider standard project risks such as resistance to change; people issues; budget overruns; access to resources, etc. when planning an IT Data Center project.

For more information

If you're interested in more information about risk assessment and ITIL service delivery, please feel free to contact us at BMC Software. We are experts on ITIL and will be happy to answer any questions you have.