IT RISK MANAGEMENT FRAMEWORK & PROCESS FOR ITSM ENVIRONMENTS

Dealing with risk is an important part of deploying new services in an IT Service Management environment (ITSM). IT risk can occur in several areas during service delivery, including operational, legal, and financial risks.

Besides minimizing problems in service delivery, many government and regulatory agencies also routinely review organizational risk management policies and responses. Implementing and controlling risk in an ITSM environment is not only smart business; it can also be a regulatory requirement.

IT risk management is a continuous process that has its own lifecycle. Although experts differ on what steps are included in the process, a simple IT risk management process usually includes the elements shown in figure 1.

Figure 1: A Simple IT Risk Management Process

Let's look at the steps involved in managing risk in an ITSM environment using an Information Technology Infrastructure Library (ITIL) framework.

1. *Identification* – Specific organizational risks should be identified whenever an item will be added to the service catalogue or when an existing service catalogue item is going to be modified. Risk identification ideally occurs in the *Service Design* phase or the *Continual Service Improvement* phase of the ITIL framework, where new services are defined and committed to. There are several ways to identify risks in rolling out a new service catalogue feature, including:
    - *Brainstorming* – Bring together all the stakeholders who have an interest in the successful implementation of the new service item and categorically review the risks that might be encountered when offering that item. Brainstorming sessions should include not only the IT department, but department heads, service desk personnel, and other supporting personnel involved with the proposed service.
    - *Organizational historical records* – Risks for new service catalogue items may parallel risks for existing items. If you're running an ITSM application such as BMC Remedy 9, you can audit service tickets for items relating to services similar to what you're planning to offer. Service tickets in products like Remedy often contain a database of realized risks that may help you discover possible risks for new IT services.
    - *Internet search, blogs, forums, commercial products, and networking* – Risks for new services can also be identified by searching the Internet for the proposed service type and its related problems. You may also find information about possible risks in blog posts, forums, commercial products discussing the service (especially e-books or seminars), or by networking with other organizations that have implemented similar services

    Risk identification should always include a description of the risk and the potential impact that will occur if the risk is realized. Potential impacts should be scored as to whether each risk carries a potential high, medium, or low impact on the business. Scoring impacts will help you decide what (if any) resources, you should allocate to addressing each risk.
2. Probability of risk occurring and prioritizing risks – It's important to determine the probability that a risk will occur as well as the importance of each risk. Probabilities can also be classified in simple terms such as a low, medium, or high probability. Take for example, a new service to provision cell phones where you may identify the following risks and their probabilities of occurring.

- *Cell phone hardware doesn't work (low probability)* – Cell phones don't usually fail right out of the box but it does occasionally happen
- *Mistake in configurations (medium probability)* – The user receives their new cell phone and a company app was not loaded on the phone or the phone is misconfigured, causing a return and reconfiguration
- *Damage to phone (high probability)* – The phone is damaged in shipment or the user does something stupid like dropping their phone in the toilet or placing it on the roof of their car and driving away, causing loss of phone and additional costs for replacement

Determining the probability of each risk occurring helps prioritize which risks you'll need to develop response plans for (see next section) and the order in which each response plan should be developed.

3. *Risk response planning* – How will your service desk and IT department respond if any of the identified risks occur? IT departments can generally create a response plan for dealing with risks by using one of the following techniques.
   - *Avoidance* – Structuring IT service delivery to avoid having the risk. To avoid cell phone configuration mistakes for example, a second tech might be required to run through a checklist verifying that all configuration items were executed correctly before delivering the phone.
   - *Mitigation* – Changing the service delivery to minimize the effects of a realized risk. Using our cell phone example, phone damage issues can be mitigated by purchasing newer water-proof phones and cases, insurance, or by using a hardened case and display cover.
   - *Planned contingency* – Having a plan to address risk when it occurs. If a new cell phone fails or is damaged, an organization might stock spares to deploy immediately as replacements.
   - *Shifting the risk* – For cell phone repair or replacement issues, the organization could have insurance or retain a third-party for repair.
   - *Acceptance of risk* – If there are risks that are not covered by avoidance, mitigation, planned contingency, or risk shifting, organizations may accept these as too cumbersome or expensive to control and leave out of the response plan.
4. *Monitoring* – It's important to monitor and identify risk triggers that activate a response. The trigger for cell phone issues would probably be a user support call. For operational support, organizations can install performance and availability monitoring software such as BMC's TrueSight Operations Management products. Monitoring software can automatically alert on-call IT responders when issues are detected.
5. *Improvement* – When new risks are identified, they should be evaluated in the context of the established management process and reflected in an updated risk management plan. In the ITIL framework, improvement is implemented under the *Continual Service Improvement* practice of the ITIL Service Lifecycle.

There's one other step in the IT risk management process that's implied but not listed here: documentation. It's important to document realized risks and their responses as they occur for two reasons: 1) It helps you implement future needs in addressing the risk *and* 2) It provides an historical record for providing documentation to auditors and regulatory agents that you have a risk management plan and are using it.