Risk Assessment / Risk Management

What is Risk Assessment / Risk Management

"Risk management is the application of risk management methods to information technology in order to manage IT risk, i.e.: The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise or organization." http://searchcompliance.techtarget.com/definition/risk-management.

There are three high-level steps to risk assessment and management:

1. **Identification of possible risks.** Once the scope of the risk assessment is determined, the next step is to gather risks or perceived risks. In this part of the process, it is good to think of everything. These risks could be from internal sources or external forces or factors. Internal sources and could include processes, gaps in policy, deficits in resourcing, change in leadership, project priorities or anything that puts the project or asset that is being assessed at risk. External factors could be new laws or regulations, political opinions, company, organization focus, additional competition, infrastructure gaps or anything that is coming from outside the project or organization that may impact the success of the project.
2. **Assessment of the risks.** This step usually involves setting up at least two tiers of assessment criteria.
    a. The first is quantifying the impact if the risk happened. For example if a risk is that a flood will impact the wiring for our server. An impact assessment would need to identify the monetary loss of the physical equipment and the loss due to inability to use that equipment to support business processes. In general, organizations create tiers of impact such as High, medium and low and define those levels.
    b. The other way that the risks are generally assess are based on probability of the risk happening. Again, scales are usually created to designate what is high, medium or low probability. In the case of the flood impacting the wiring of the project's server. This may be a low probability as the server room has only been impacted by high water once in the last ten years. Or it can be a high probability if it has happened more than once in the last year.
    c. Once the risks are quantified and the assessment on probability has been made, the next step is to prioritize which risks to address, mitigate or manage. There could be a decision that low impact and low probability risks are known, but not addressed. On the other hand, high impact and high probability risks will need to have an action plan. The organization will need to determine what to do with the risks in the middle scales.
3. **Mitigations / Management.** Once you have an idea of which risks are impactful and most probable, the next step is to determine an action plan for reducing (mitigating) the risk. When creating an action plan, it is best to set specific steps and timeframes for reducing the risks. When developing mitigations, keep the impact and probability in mind.
4. **Review and Manage.** After a mitigation plan is in place, it is recommended that there is a process to review the status of mitigations, identify and assess new risks, and update assessments based upon new information and status of mitigations. This should occur on a regular basis.

When to Use Risk Management

Risk management practices and methods can be used in the following ways:

- Assessment and management of risk for a specific topic like privacy or security.
- Assessment and management of risks during the lifecycle of a project.
- Assessment of risks when creating a Business Continuity Plan for continuing business after a disaster or crisis that has impact on electricity, internet availability, server use or software use.

Tools, Templates and Resources

The following templates and tools may help you with this process.

https://hingx.org/Risk%20Assessment%20Toolkit

Risk-Assessment-Template.xlsx