NAVEX™

Datasheet

How to Get Started With IT Risk Management

6 Core Components of a Proactive Process for Mitigating and Managing Risks

The job of an IT leader and cybersecurity professional may seem straightforward, but in reality, this is rarely the case. Even with the best intentions, complications frequently come at the worst possible time.

Many IT leaders struggle with taking a reactive stance to issues instead of serving in a more strategic role. Taking a passive or reactive approach to risks can lead to detrimental consequences to the business.

Some of the following scenarios may sound familiar:

- The need to put out fires for things that seem trivial on the surface but could be problematic for both the IT unit and the company in general. These issues can be borne internally, or they can originate from challenges in the external market or operating environment.
- Last-minute requests and unplanned projects divert attention at critical times.
- IT is faced with doubts on whether it is focusing human and financial resources on the right things.
- Programs are run on spreadsheets, or through disjointed systems.

Finding a solution to this problem is critical to ensuring IT plays a helpful role in moving the company forward.

After all, technology is the backbone of any business in today's world. It has become so ubiquitous that without a well-oiled tech infrastructure, a company will come to a grinding halt.

In fact, any IT function that is unable or unprepared to support their company's tech needs will, in reality, hold it back from achieving strategic goals – or worse, lead to its eventual demise. This reliance creates additional vulnerabilities companies need to consider.

Therefore, it is critical to take methodical steps to address vulnerabilities and position IT to play its natural and valuable role to help the company accomplish its goals and ultimately succeed.

While there are plenty of generalized standards or guidelines to address risk and deliver technology services, these standards do not account for a company's unique culture and needs. Without knowing the company's specific attributes, it is impossible to provide a complete template or blueprint to mitigate and manage specific IT risks. However, there are universal components or steps of a risk management framework regardless of the type of risks your business focuses on to help get organizations started quickly and simply.

Each of the following six components or steps in this framework builds on the last, which is why it is vitally important to complete each step before moving on to the next.

Components of an IT Risk Management Framework

1 Establish the context

The "context" of an organization's risk management efforts simply means identifying your focal point, which can range from anything from strategic planning to a one-time project. In the case of IT, the context can include anything from the company-wide technology strategy to specific topics like cybersecurity and privacy to processes such as Software Development Life Cycle (SDLC) or User Access Management (UAM).

2 Risk Identification

Now that you have pinpointed the "context" under discussion, it is time to identify the actual risks linked to that context. To do this effectively, you need to determine the approach you will use. The best approach and technique will depend upon the context. Examples include:

- **Interviews** – best for understanding major risks from the viewpoint of executives and high-level managers.
- **Scenario analysis** – helpful during the strategic planning process for identifying high impact yet low probability risks.
- **Surveys** – useful for identifying multiple risks across the organization due to sheer volume of participants. (Sometimes this method can be surprisingly effective.)
- **Root Cause Analysis** – helpful for identifying the underlying cause(s) of known issues. This information can then be used to identify common root causes across multiple risk events.

Do not feel restricted to using only one method – in fact, it can be detrimental to long-term efforts to only rely on one method in all circumstances. A healthy mix of identification methods based on the context and participants in each situation will help ensure you end up with a robust, but accurate, list of risks.

3 Risk Assessment

While the risk identification phase is crucial for understanding threats and opportunities, a risk management process that protects and enhances value is about more than a list.

The assessment phase helps IT teams and decision makers learn which risks are important and how they connect to the context. Neglecting this phase can lead to even more wasted resources and problems than doing nothing at all. Many of the methods for gathering information for an assessment are much the same as those outlined in the identification phase. However, there are two major additions to the list: workshops (small groups of people from the business areas to be facilitated during the assessment discussion), and quantification (helpful when you already have data elements that can be obtained, analyzed, and modeled).

At its most basic level, risk assessment only considers two elements: the likelihood (or probability) of the risk occurring and the impact should it occur. More established risk processes may consider velocity, pervasiveness, and even the interdependency of risks.

The parameters used to evaluate this will depend on your company's needs and experience level, but one important thing to keep in mind – taking too broad a view will make it difficult to identify issues and solutions, while being too detailed can lead to no progress being made.

4 Risk Analysis

It may seem like risk assessment and analysis are one in the same, but they are not. The former focuses on individual risks, while the latter dives into "the big picture" to determine the right risks to focus on.

Time and financial resources are limited, and trying to focus on all risks simultaneously can lead to stagnation and information overwhelm.

The analysis step takes information from the assessment and analyses it using different tools like risk appetite, tolerance, and others. For risks exceeding the company's risk appetite, a root cause analysis can be done to address the ultimate source of uncertainty. While it is possible that nothing can be done about the risk itself, it may be possible to address the root cause and therefore reduce the chance of it occurring.

The goal of this analysis step is to ensure you are focusing on the right risks at the right time for maximum value to the organization.

5 Risk Response

Once risks are analyzed and prioritized, it is time to determine the right response. Specific response options include:

- **Avoid** – if there is absolutely zero tolerance for a specific risk, it is best to avoid it. For example, if the business is considering a different software, but determines the changeover could put highly sensitive data at risk for compromise or exposure from a cyber-attack. If this risk is too intolerable, you may decide to cancel the change and therefore avoid this risk.
- **Mitigate or reduce** – if a risk is slightly above what IT or the company is willing to tolerate, steps can be taken to reduce the likelihood, or impact – or both to bring the risk to within acceptable limits.
- **Transfer** – this response does not eliminate or reduce the chance of a risk occurring, but rather delegates or transfers responsibility to a third-party. Insurance is the most common way of doing this, as commonly done for data breaches, but indemnification clauses are another method. Either way, the goal is to make the company whole should the risk materialize.

- **Accept** – sometimes there are risks that you are unable to avoid, reduce, or transfer, or it is simply not worth the trouble. Many strategic type risks will fall into this category since companies must be willing to take risks to survive and thrive in today's tumultuous world.

6 Risk Monitoring and Reporting

After risks are identified and assessed, and a response is determined, the next step is ongoing risk monitoring and reporting.

With an ever-changing risk landscape, this is a vital part of IT risk management. In the event the impact, likelihood, and the nature of the risk goes outside acceptable levels, it's imperative to act quickly to ensure the risk does not become unmanageable. It is not necessary, nor practical, to monitor each and every risk, but risks that are close to or exceed the company's tolerance much be continuously monitored.

It is also likely some risks will impact other departments or the corporate/IT strategy. Therefore, reports may need to be prepared to alert other business on any actions being taken.

As a part of Board oversight, they will need to be made aware of risks the company faces and how they are being addressed. Increased scrutiny from investors, regulators and the public have transformed IT risk management from "nice to have" to "must-have".

Conclusion

IT risk management is a continuous process – there is no endpoint.

Whether your risk program currently utilizes spreadsheets or works within a digital solution, the steps above should guide your decisions about solution capabilities. IT risk management involves many stakeholders, and an automated, digital capability should be established that is easy to deploy and agile to evolve as the risk program matures and company needs change. Once the appropriate solution is identified, it is time to deliver efficiency and value to the program and organization.

The six components above make up a robust risk management process aimed at helping the IT unit and company at-large proactively identify, assess, and respond to risks.

Developing a robust and comprehensive IT risk management process requires trial and error, so do not be surprised if the first try isn't the most optimal approach. However, developing an efficient process delivers tremendous value to both the IT Department and the company as a whole.