

3 Things About IT Risk Management - Ideas, Strategies, and Tips

[Starting an IT business](#) is already a huge project itself. And when it comes to huge projects, [project management](#) is a necessity. If you're planning to open your own IT company soon, you should know that there are significant risks involved in doing so. For that reason, risk management is just as important as project management. These risks are things you must look into because they can cause major losses and damages. However, these risks should not hinder you from running your IT company. Here are things you need to know about risk management in the IT industry.

Types of Risks

Cyber Risks

Cyber risks are incidents that concern the attack of a company's computer systems. These could disrupt their computerized operations and may lead to the leak of important and confidential information and data. These incidents are called cyber-attacks. Any company, including those outside the IT industry, are at risk of cyber-attacks if they have computer systems, especially those with suboptimal [IT security](#) protocols. Cyber risks are considered as among the most alarming dangers for every business. According to an article by Devon Milkovich in CybintSolutions.com, small businesses are the targets of 43% of cyber-attacks. And 60% of these small businesses, based on a stat from Fundera.com, close six months after. That said, your IT business is still considered as a small business, even if it is in its startup phase. It means that the company can be very vulnerable to cyber risks.

Operational Risks

Operational risks are concerns or dangers that might occur in the middle of operations. These types of risks are never out of the equation. Some of them can even be imminent if left unchecked. The types of incidents that might arise in operational risks depend on how you run the operations of your IT business. Operational risks include accidents in the workplace, external and internal fraud, employees breaching company rules and [policies](#), and many more.

Legal Risks

As the name implies, legal risks are issues that involve legalities with direct ties to legislative laws and regulations. These types of risks should be of major concern because they can affect the credibility and reputation of your IT business. Other than that, legal risks can turn your financial assets to liabilities. External entities can file legal charges and lawsuits to a company for specific reasons. The best thing you can do to minimize legal risks is to follow the laws and regulations in running your IT company.

Natural Disasters

Natural disasters are inevitable because we can't control nature, and this may affect your company. When it comes to dealing with the risks of natural disasters, the best thing that companies should do is to be prepared for them. Hurricanes, floods, earthquakes, and tornadoes are among the most common natural disasters. Nevertheless, there are insurances to protect your business's assets from the aftermath of natural disasters. They cover every [cost estimation](#), or at least most of it, for businesses to recover.

Security Risks

Security risks are always looming around. Many outside forces might want to illegally breach the vicinity of a company for their own gain. These forces can put you out of business. Theft, fraud, and confidential information leakage are primary examples of security risks, including cyber risks, which we've discussed earlier.

Why Is Risk Management Important?

Without a proper and standardized risk management protocol, a company is highly vulnerable to dangers and incidents that can derail its operations, assets, and every foundation that keeps it standing. It'll be like a carcass for vultures. Risk management procedures will eliminate or at least regulate risks for the protection of a business. With an established risk management protocol, the progress and future of your company will be stable and secure. Other than that, it allows for a much safer working environment for the employees.

How to Implement Risk Management - 5 Steps

These are the steps you can apply to establish a risk management protocol for your IT company.

Identify Risks

At the very beginning of the risk management process, you must identify the risks first. You can't prepare for something if you don't know in the first place what you'll be dealing with. In this case, you have to do an [analysis](#) of the components of your IT business to determine what sort of risks it might encounter in the future.

Risk Assessment

Once you've identified the possible risks, assess them thoroughly. Try to calculate how they might arise or escalate. By doing so, you can formulate specific procedures to avoid these risks, or to eradicate them if possible. Among the dangers your IT business could encounter are during software product releases. In such an event, external forces might want to steal your product or copy it in some way. To come up with ways to counteract that, you have to conduct a software release risk assessment.

Evaluate Risk

The next step is to evaluate the possible risks. Evaluate them by studying how much damage they can cause to your company. In this way, your company will know how to be prepared when such risks will occur. In other words, you'll have a checklist of possible contingencies.

Develop Response Plans for the Risks

Of course, you should do appropriate actions to counteract the damages of possible risks when they happen. For that reason, you have to develop a risk response plan. It'll serve as a standard guide on how to minimize damages caused by risks and to put your business back on its feet. In addition, every employee must know the risk response plan so that they'll know what to do.

Monitor and Review Risk

During the course of operations, you have to constantly monitor and review possible risks despite the presence of response plans. Remember that the main objective of risk management is to keep risks at bay as much as possible. Simply put, you have to keep an eye at them all the time. You can assign specific employees to submit a [daily report](#) of their work to see if there are things that need to be monitored meticulously for precautions.

Tips for Risk Management

Here are five tips you can apply in conducting risk management procedures.

Establish Protocols for Safeguarding Information

The information that your company relays internally must be protected at all costs. They are confidential and must not be leaked or taken by external entities. Therefore, you have to safeguard them by establishing a suitable information security protocol.

Create Emergency Response Plans

The scope of a risk [management](#) plan doesn't stop in avoiding possible dangers and incidents. It should also extend when such dangers and incidents arise in the form of an emergency response plan. With an emergency response plan, the personnel of your IT company will know what they must do to counteract the damages of major risks; thus, reducing the possibility of panic. Your personnel must also study and practice the established emergency response plan.

Know Policies and Procedures

One of the effective approaches to optimize a risk management plan is simply knowing and following the policies and procedures. They are present for many good reasons, aside from just standardizing the IT service and production procedures of your company. Policies and procedures were formulated for safety purposes in the first place.

Have a Clear Communication

To keep risks at bay as much as possible, you need the cooperation of your colleagues. And when it comes to cooperation, having clear communication is necessary. With clear communication, you and your colleagues can collaborate easily in managing risks. Every bit of crucial information must be concise and accurate.

Evaluate Early and Often

When a certain risk is detected, no matter how small it is, you have to evaluate it immediately. You'll never know when and how it might escalate and cause damages to your IT business. Also, you have to do [risk analysis](#) as often as possible for absolute precaution.

Performing risk management procedures is like being a weatherman. You monitor possible and imminent bad weather conditions and prepare for it before they arrive. Risk management is specifically challenging in the IT industry because of the involvement of digital technology. However, the risks are manageable if you simply invest effort and time to reinforce your risk management practices. With a reinforced risk management plan, your IT company's future is secure and bright.