

IT Risk Assessment



Contents

Contents.....	2
Introduction.....	3
What benefits accrue from an IT risk assessment?.....	3
Conducting an IT Risk Assessment.....	4
Common Pitfalls to Avoid.....	5
Our solution for conducting an efficacious IT Risk Assessment.....	5
Conclusion.....	5
About the Author.....	6



Introduction

A 2014 study by the Ponemon Institute and HP showed that the average annual cost of cyber crime incurred by U.S. organizations has risen by 96% between 2010 and 2014, to a staggering \$12.7 million. All organizations are aware of the danger posed by hackers out to steal data and money, and yet, many fail to keep their security policies and systems updated. Outdated software with vulnerabilities and practices that leave the organization open to threat are still common. In order to protect your organization, you must methodically evaluate the risks, threats, and vulnerabilities surrounding your IT infrastructure. In short, you need an **IT Risk Assessment**.

An IT Risk Assessment is a comprehensive review of the IT organization, with the objective of identifying existing flaws that could be exploited to threaten the security of the network and data. It serves as the basis for deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization.

What benefits accrue from an IT risk assessment?

An IT risk assessment does more than just tell you about the state of security of your **IT infrastructure**; it can facilitate decision-making on your organizational security strategy. Some of the benefits of conducting an IT risk assessment are:

Identify security threats and vulnerabilities

Conducting an IT risk assessment can help locate vulnerabilities in your existing IT infrastructure and enterprise applications, before these are exploited by hackers. Appropriate action can then be taken to patch and fix these vulnerabilities, reducing IT risk and the potential impact of any breach.

Identify the maturity level of existing security controls and tool usage

An IT risk assessment can help evaluate the existing defenses and preventive / corrective controls in place. The identified areas of improvements can then be mapped against the current technology landscape to ascertain if improvements are possible (additional security controls or a possible correlation of data arising from these controls that can result in advanced threat intelligence, for instance). The IT assessment thus highlights remediation measures to maximize current investments.

Enhance enterprise-wide security policies

Not only will the assessment help plug holes in your security, but, by tying IT risk to enterprise-wide risk management, it can help create more secure solutions, practices and policies within the organization. This will improve the overall security of information in the organization, and help identify what security strategy best suits your organization.

Gauge security awareness and readiness

An IT risk assessment needs the involvement of various **IT security** personnel, as well as other employees and managers, which will help you gauge how aware various individuals and departments are of security threats, vulnerabilities, practices and solutions. It also gives a measure of how well the employees and contractors understand and follow the enterprise's security policies and standards. An IT risk assessment may thus, point to the need for security awareness campaigns or workshops for your employees.

Justify security investments

Reviewing existing IT infrastructure and studying the potential business impact of a compromised system can help make a business case for security spending. An assessment can present a fair analysis of security investment versus potential losses and costs from security breaches.

Prove security due diligence

With IT risk assessment regulations likely to come into play in the next few years, it is important that your organization have documented proof of conducting assessments on a regular basis. Moreover, if you have insurance that deals with data loss, the insurance organizations will demand proof that the appropriate security measures were in place (in case of an incident). IT risk assessment documentation can help prove that.

Understand the security maturity of your partners

A recent study by PwC has found that the biggest challenge to security today is from internal (employees and partners), not external threats. A robust IT assessment includes assessment of security measures within your partner network. Findings from the assessment can help plan better defenses against third-party attacks.

The overall objective of an organization's security strategy is to ensure the protection of information (whether its own or that of customers, suppliers, and other parties) and assets. An IT risk assessment is a major preventive measure that actively mitigates the risk of vulnerabilities and threats negatively impacting the organization.

Conducting an IT Risk Assessment

A traditional IT risk assessment reviews IT-related issues such as outages, application downtime and hardware failures. It comprises three main steps:

Evaluation

The evaluation phase focuses on understanding the critical resources that may be affected by the threat or vulnerability. Business evaluation can be conducted by:

Identifying critical business processes and assets: The first step is to identify all the information, processes, and information assets that are crucial or important for the functioning and security of the business. Identifying these critical components will help you decide what you want to protect, and what the consequence of losing them would be.

Identifying vulnerabilities: A proactive review process to check for inherent vulnerabilities that could be exploited and affect the organization. When identifying vulnerabilities, remember to view them within the context of the business, i.e. how they will affect your business as a whole.

Gathering information on potential threats to your organization's information: Knowing what threats each of your IT assets may face and from where those may originate can help formulate a plan of defense.

Risk Assessment

The risk assessment phase consists of determining the likelihood and the severity of threats and vulnerabilities. Not all threats are equal—some happen more often than others, and others are more devastating to the organization's infrastructure. The first step in identifying the worst threats is to find out how likely it is that the threat will occur. Next, quantify the impact the threat could have on the enterprise. Then, by mapping threats and vulnerabilities, likelihood, and impact to critical information, processes, and information assets, you can determine a scale to rate the severity of the consequences of an event or a breach in security. This will help determine which threats or vulnerabilities you need to prepare for.

Risk Mitigation

Risk mitigation is all about preparing to face a potential threat or tackle a possible vulnerability. It requires the organization to take many steps, either on its own, in collaboration with the IT infrastructure providers or with the aid of IT security organizations. There are three measures your organization must have in place:

- **Preventive:** Preventive measures identify threats before they occur. These notify your security team when they spot a threat or locate vulnerability, so they can begin taking steps to deal with the event.
- **Mitigation:** Mitigation aims to reduce or minimize the consequences of an event or breach of security. These measures ensure that the threat does not impact the entire infrastructure or all the information resources.
- **Recovery:** Recovery operations enable the organization to resume business activities post the event. This includes recovering data from remote/offsite data centers and getting systems up and running in safe environments.

Common Pitfalls to Avoid

There are some common pitfalls that you should be aware of that can weaken the efficacy of an IT risk assessment:

Viewing IT risk assessment as separate from enterprise risk management: IT risks cannot be treated as a discrete aspect of security not related to the wider enterprise. Incorporate IT risk management into the enterprise risk management system in order to understand how

IT risks affect and are affected by other security and business risks.

Their broader impact on the whole organization must be considered.

Conducting a non-contextual assessment:

IT risk assessments must be viewed within a business context. When analyzing breaches and vulnerabilities, it is essential to see these in the context of your information assets and how an attack on them will impact business. This kind of in-depth and actionable analysis will help develop an effective assessment that provides a window into not only technology flaws, but also business vulnerabilities.

Diluting the focus on assets that matter: The aim should not be to audit every IT equipment, server, or application, but to conduct a thorough assessment with greater frequency for targeted, high-risk IT assets.

Ignoring third-party risk: While organizations account for risk from organization practices and software, they often forget to account for risks from other third-party organizations and individuals. In reality, these latter risks play a significant role, especially if your enterprise systems or financial exchange systems are integrated, since a breach of your vendor's network can compromise your own data.

Improper assessment of threats: Some organizations fail to account for the severity of threats, or broadly classify threats into categories; both these practices lead to an insufficient understanding of the real danger from each threat.

Infrequent assessment of risks: Risk assessment cannot be a once-a-year activity; it is a continuous process requiring frequent checks.

Imbalance in assessment parameters: IT risk assessment is not a list of items to be rated, it is an in-depth look at the many security practices and software. Many organizations fail to realize that there should be a balance between the quantitative and qualitative data collected for assessment.

Relying mostly on automated assessment tools: While automated tools facilitate efficient assessment and a continuous monitoring of IT assets and infrastructure, manual pen testing is required for a more in-depth and comprehensive assessment. Some risks, specifically business vulnerabilities, can only be identified by manual intervention.

Inability to translate the findings into actionable items: Translating the findings into a set of actionable and remediation plans, and aligning them with IT strategy and roadmap is a key step that is often left incomplete after an IT risk assessment. Bringing the senior management into loop and getting their buy-in on remediation plans and regular follow-ups are key to realizing the full benefit of the assessment.

Conclusion

Our solution for conducting an efficacious IT Risk Assessment

Happiest Minds' [ComplianceVigil](#) is a solution for monitoring and managing IT risks. It provides a platform for risk and compliance management where framework, management, automation and monitoring are bundled into a single platform delivered from the cloud (private or public). ComplianceVigil will provide your organization with an integrated and flexible framework for documenting and assessing risks and their impacts, managing audits, and planning solutions.

About the Author



Priya Kanduri

Heads the Risk and Compliance practice at Happiest Minds Technologies Pvt. Limited. She brings in more than 15 years of experience in the area of IT Security across multiple domains like **Identity and Access Management**, Data Security, Cloud Security, Governance, Risk and Compliance. Her recent work includes running large information security programs for enterprises across UK and Europe and helping them get compliant with regulatory mandates. She is a regular speaker at security conferences on various subjects like identity management & governance, IP protection, risk management and cloud adoption for compliance.

Happiest Minds

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable **digital transformation** for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and **security services**. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

© Happiest Minds. All Rights Reserved.
Business Contact: business@happiestminds.com
Visit us: www.happiestminds.com

Follow us on



This Document is an exclusive property of Happiest Minds Technologies.