netwrix

IT Risk Assessment Checklist

Identify your risks to jump-start an A-class risk mitigation program

What is IT risk assessment?

With threats to sensitive data growing in both number and sophistication every day, organizations cannot afford a scattershot approach to security. Instead, they need to focus their limited IT budgets and resources on the specific vulnerabilities in their unique security posture.

To do this, they need to identify, analyze and prioritize the risks to the confidentiality, integrity or availability of their data or information systems, based on both the likelihood of the event and the level of impact it would have on the business. This process is called IT risk assessment.

Risk assessment is primarily a business concept and it is all about money. You have to first think about how your organization makes money, how employees and assets affect the profitability of the business, and what risks could result in large monetary losses for the company. After that, you should think about how you could enhance your IT infrastructure to reduce the risks that could lead to the largest financial losses to organization.

Basic risk assessment involves only three factors: the importance of the assets at risk, how critical the threat is, and how vulnerable the system is to that threat. Using those factors, you can assess the risk—the likelihood of money loss by your organization. Although risk assessment is about logical constructs, not numbers, it is useful to represent it as a formula:

Risk = Asset X Threat X Vulnerability

Although risk is represented here as a mathematical formula, it is not about numbers; it is a logical construct. For example, suppose you want to assess the risk associated with the threat of hackers compromising a particular system. If your network is very vulnerable (perhaps because you have no firewall and no antivirus solution), and the asset is critical, your risk is high. However, if you have good perimeter defenses and your vulnerability is low, and even though the asset is still critical, your risk will be medium.

There are two special cases to keep in mind:

- Anything times zero is zero. If any of the factors is zero, even if the other factors are high or critical, your risk is zero.
- Risk implies uncertainty. If something is guaranteed to happen, it is not a risk.

Why do you need IT risk assessment?

- IT risk assessment should be the foundation of your IT security strategy to understand what events can affect your organization in a negative way and what security gaps pose a threat to your critical information, so you can make better security decisions and take smarter proactive measures.

- IT risk assessment helps you determine the vulnerabilities in information systems and the broader IT environment, assess the likelihood that a risky event will occur, and rank risks based on the risk estimate combined with the level of impact that it would cause if it occurs.

- IT risk assessment is required by many compliance regulations. For instance, if your organization must comply with HIPAA or could face GDPR audits, then information security risk assessment is a must-have for your organization in order to minimize the risk of noncompliance and huge fines.

STEP #1

Collect the information you need to assess risks. Here are a few ways to do it:

- ✔ Interview management, data owners and other employee
- ✔ Analyze your systems and infrastructure
- ✔ Review documentation

STEP #2

Find all valuable assets across the organization that could be damaged by the threats. Here are just a few examples:

- ✔ Servers
- ✔ Website
- ✔ Client contact information
- ✔ Trade secrets
- ✔ Customer credit card data

Because most organizations have a limited budget for risk assessment, you will likely have to limit the scope of the project to mission-critical assets. Accordingly, you need to define a standard for determining the importance of each asset. Common criteria include the asset's monetary value, legal standing and importance to the organization. Once the standard has been approved by management and formally incorporated into the risk assessment security policy, use it to classify each asset you identified as critical, major or minor.

STEP #3

Identify potential consequences. Determine what harm the organization would suffer if a given asset were damaged. This is a business concept, the likelihood of financial or other business losses. Here are a few consequences you should care about:

- **Legal consequences.** If somebody steals data from one of your databases, even if that data is not particularly valuable, you can incur fines and other legal costs because you failed to comply with the data protection security requirements of HIPAA, PCI DSS or other compliance.
- **Data loss.** Theft of trade secrets could cause you to lose business to your competitors. Theft of customer information could result in loss of trust and customer attrition.
- **System or application downtime.** If a system fails to perform its primary function, customers may be unable to place orders, employees may be unable to do their jobs or communicate, and so on.

STEP #4

Identify threats and their level. A threat is anything that might exploit a vulnerability to breach your security and cause harm to your assets. Here are a few common types of threats:

- **Natural disasters.** Floods, hurricanes, earthquakes, fire and other natural disasters can destroy much more than a hacker. You can lose not only data, but the servers and appliances as well. When deciding where to house your servers, think about the chances of a natural disaster. For instance, don't put your server room on the first floor if your area has a high risk of floods.
- **System failure.** The likelihood of system failure depends on the quality of your computer For relatively new, high-quality equipment, the chance of system failure is low. But if the equipment is old or from a "no-name" vendor, the chance of failure is much higher. Therefore, it's wise to buy high-quality equipment, or at least equipment with good support.
- **Accidental human interference.** This threat is always high, no matter what business you are in. Anyone can make mistakes such as accidentally deleting important files, clicking on malware links, or accidentally physical damaging a piece of equipment. Therefore, you should regularly back up your data, including system settings, ACLs and other configuration information, and carefully track all changes to critical systems.
- **Malicious humans.** There are three types of malicious behavior:
  - **Interference** is when somebody causes damage to your business by deleting data, engineering a distributed denial of service (DDOS) against your website, physically stealing a computer or server, and so on.
  - **Interception** is classic hacking, where they steal your data.
  - **Impersonation** is misuse of someone else's credentials, which are often acquired through social engineering attacks or brute-force attacks, or purchased on the dark web.

STEP #5

Analyze Controls. Analyze the controls that are either in place or in the planning stage to minimize or eliminate the probability that a threat will exploit vulnerability in the system. Controls can be implemented through technical means, such as computer hardware or software, encryption, intrusion detection mechanisms, and identification and authentication subsystems. Nontechnical controls include security policies, administrative actions, and physical and environmental mechanisms.

Both technical and nontechnical controls can further be classified as preventive or detective controls. As the name implies, preventive controls attempt to anticipate and stop attacks. Examples of preventive technical controls are encryption and authentication devices. Detective controls are used to discover attacks or events through such means as audit trails and intrusion detection systems.

STEP #6

Identify vulnerabilities and assess the likelihood of their exploitation. A vulnerability is a weakness that allows some threat to breach your security and cause hard to an asset. Vulnerabilities can be physical, such as old equipment, or a problem with software design or configuration, such as excessive access permissions or unpatched workstations.

Vulnerabilities can be identified through vulnerability analysis, audit reports, the NIST vulnerability database, vendor data, commercial computer incident response teams, and system software security analysis.

Testing the IT system is also an important tool in identifying vulnerabilities. Testing can include the following:

- Information Security test and evaluation (ST&E) procedures
- Penetration testing techniques
- Automated vulnerability scanning tools

You can reduce your software-based vulnerabilities with proper patch management. But don't forget about physical vulnerabilities. For example, moving your server room to the second floor of the building will greatly reduce your vulnerability to flooding.

STEP #7

Assess the Impact a Threat Could Have. Impact analysis should include the following factors:

- The mission of the system, including the processes implemented by the system
- The criticality of the system, determined by its value and the value of the data to the organization
- The sensitivity of the system and its data

The information required to conduct an impact analysis can be obtained from existing organizational documentation, including a business impact analysis (BIA) (or mission impact analysis report, as it is sometimes called). This document uses either quantitative or qualitative means to determine the impact that would be caused by compromise or harm to the organization's information assets.

An attack or adverse event can result in compromise or loss of information system confidentiality, integrity and availability. As with the likelihood determination, the impact on the system can be qualitatively assessed as high, medium or low.

The following additional items should be included in the impact analysis:

- The estimated frequency of the threat's exploitation of a vulnerability on an annual basis
- The approximate cost of each of these occurrences
- A weight factor based on the relative impact of a specific threat exploiting a specific vulnerability

STEP #8

Prioritize the Information Security Risks. For each threat/vulnerability pair, determine the level of risk to the IT system, based on the following:

- The likelihood that the threat will exploit the vulnerability
- The impact of the threat successfully exploiting the vulnerability
- The adequacy of the existing or planned information system security controls for eliminating or reducing the risk

A useful tool for estimating risk in this manner is the risk-level matrix. A high likelihood that the threat will occur is given a value of 1.0; a medium likelihood is assigned a value of 0.5; and a low likelihood of occurrence is given a rating of 0.1. Similarly, a high impact level is assigned a value of 100, a medium impact level 50, and a low impact level 10. Risk is calculated by multiplying the threat likelihood value by the impact value, and the risks are categorized as high, medium or low based on the result.

STEP #9

Recommend Controls. Using the risk level as a basis, determine the actions that senior management and other responsible individuals must take to mitigate the risk. Here are some general guidelines for each level of risk:

- **High**— A plan for corrective measures should be developed as soon as possible.
- **Medium** — A plan for corrective measures should be developed within a reasonable period of time.
- **Low** — The team must decide whether to accept the risk or implement corrective actions.

As you consider controls to mitigate each risk, be sure to consider:

- Organizational policies
- Cost-benefit analysis
- Operational impact
- Feasibility
- Applicable regulations
- The overall effectiveness of the recommended controls
- Safety and reliability

STEP #10

Document the Results. The final step in the risk assessment process is to develop a risk assessment report to support management in making appropriate decisions on budget, policies, procedures and so on. For each threat, the report should describe the corresponding vulnerabilities, the assets at risk, the impact to your IT infrastructure, the likelihood of occurrence and the control recommendations. Here is a very simple example:

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Control Recommendations
System failure — Overheating in server room High	Air conditioning systems is ten years old High	Servers Critical	All services (website, email, etc.) will be unavailable for at least 3 hours Critical	High Current temperature in server room is 40C	High Potential loss of $50,000 per occurrence	Buy a new air conditioner, $3,000 cost
Malicious human (interference) — DDOS attack High	Firewall is configured properly and has good DDOS mitigation Low	Website Critical	Website resources will be unavailable. Critical	Medium DDOS was discovered once in 2 years	Medium Potential loss of $10,000 per hour of downtime	Monitor the firewall
Natural disasters — Flooding High	Server room is on the 3rd floor Low	Servers Critical	All services will be unavailable Critical	Low Last flood in the area happened 10 years ago	Low	No action needed
Accidental human interference — Accidental file deletions High	Permissions are configured properly; IT auditing software is in place; backups are taken regularly Low	Files on a file share Medium	Critical data could be lost but almost certainly could be restored from backup Low	Medium	Low	Continue monitoring permissions changes, privileged users and backups

You can use your risk assessment report to identify key remediation steps that will reduce multiple risks. For example, ensuring backups are taken regularly and stored offsite will mitigate the risk of accidental file deletion and also the risk from flooding. Each of these steps should have the associated cost and should deliver real benefit in reducing the risks. Remember to focus on the business reasons for each improvement implementation.

STEP #11

Create a strategy for IT infrastructure enhancements to mitigate the most important vulnerabilities and get management sign-off.

STEP #12

Define mitigation processes. You can improve your IT security infrastructure but you cannot eliminate all risks. When a disaster happens, you fix what happened, you investigate why it happened, and then you try to prevent it from happening again or at least make the consequences less harmful.

As you work through this process, you will get a better idea of how the company and its infrastructure operates and how it can operate better. Then you can create risk assessment policy that defines what the organization must do periodically (annually in many cases), how risk is to be addressed and mitigated (for example, a minimum acceptable vulnerability window), and how the organization must carry out subsequent enterprise risk assessments for its IT infrastructure components and other assets.

Always keep in mind that the information security risk assessment and enterprise risk management processes are the heart of the cybersecurity. These are the processes that establish the rules and guidelines of the entire informational security management, providing answers to what threats and vulnerabilities can cause financial harm to our business and how they should be mitigated.

About Netwrix

Netwrix Corporation is a software company focused exclusively on providing IT security and operations teams with pervasive visibility into user behavior, system configurations and data sensitivity across hybrid IT infrastructures to protect data regardless of its location. Over 9,000 organizations worldwide rely on Netwrix to detect and proactively mitigate data security threats, pass compliance audits with less effort and expense, and increase the productivity of their IT teams.

Founded in 2006, Netwrix has earned more than 140 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com

Corporate Headquarters:
300 Spectrum Center Drive, Suite 200, Irvine, CA 92618
Phone: 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023
netwrix.com/social

Identify, Assess and Reduce IT Risks

with Netwrix Auditor

- Gain a bird's-eye view of your security posture
- Identify security gaps that require your attention
- Get actionable data about how to reduce the identified risks
- Continuously evaluate your security posture

Download Free 20-Day Trial