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.

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 starting May 2018, then information security risk assessment is a must-have for your organization in order to minimize the risk of noncompliance and huge fines.

To begin your risk assessment, take the steps listed in the following checklist. This simple checklist is just one of several tools available to conduct information security risk assessments in your organization. Once the step is complete, simply check it off.

Yes/No	Steps to take
	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
	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
	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 • Data loss • System or application downtime
	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 • Software failure • Hardware failure • Malicious human actions (interference, interception or impersonation) • Data backup failure • Power outage
	5. 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.
	6. Assess risk. Risk is the potential that a given threat will exploit the vulnerabilities of the environment and cause harm to one or more assets, leading to monetary loss.
	7. Create a risk management plan predict risks, estimate impacts, and define responses to each risk.
	8. Create a strategy for IT infrastructure enhancements to mitigate the most important vulnerabilities and get management sign-off.
	9. 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.

Learn how Netwrix Auditor can help you close security holes by identifying and prioritizing risks