What is a cybersecurity risk assessment?

A cybersecurity risk assessment is an assessment of an organization's ability to protect its information and information systems from cyber threats.

The purpose of a cybersecurity risk assessment is to identify, assess, and prioritize risks to information and information systems. A cybersecurity risk assessment helps organizations identify and prioritize areas for improvement in their cybersecurity program. It also helps organizations communicate their risks to stakeholders and make informed decisions about how to allocate resources to reduce those risks.

There are many cybersecurity risk assessment frameworks and methodologies available, but they all share a common goal.

The [National Institute of Standards and Technology (NIST) Cybersecurity Framework](https://www.itgovernanceusa.com/nist-cybersecurity-framework) is one of the most popular risk assessment frameworks. It provides a flexible and structured approach for organizations to assess their cybersecurity risks and prioritize actions to reduce those risks.

Another popular risk assessment framework is the [ISO 27001:2013 standard](https://www.itgovernanceusa.com/iso27001). This standard provides a comprehensive approach to information security management, including requirements for risk assessment and risk treatment.

Organizations can also develop their own customized risk assessment frameworks and methodologies. Whatever approach an organization chooses, the goal should be to identify, assess, and prioritize risks to information and information systems.

Why carry out a cybersecurity risk assessment?

A cybersecurity risk assessment is important because it can help identify risks to your organization’s information, networks and systems. By identifying these risks, you can take steps to mitigate or reduce them. A risk assessment can also help your organization develop a plan to respond to and recover from a cyber attack.

Organizations should conduct cybersecurity risk assessments on a regular basis to keep their risk profiles up to date. Additionally, if there are changes to an organization's computer networks or systems, a new risk assessment should be conducted.

What does a cybersecurity risk assessment include?

A cybersecurity risk assessment evaluates the organization's vulnerabilities and threats to identify the risks it faces. It also includes recommendations for mitigating those risks.

A risk estimation and evaluation are usually performed, followed by the selection of controls to treat the identified risks.

It is important to continually monitor and review the risk environment to detect any changes in the context of the organization, and to maintain an overview of the complete risk management process.