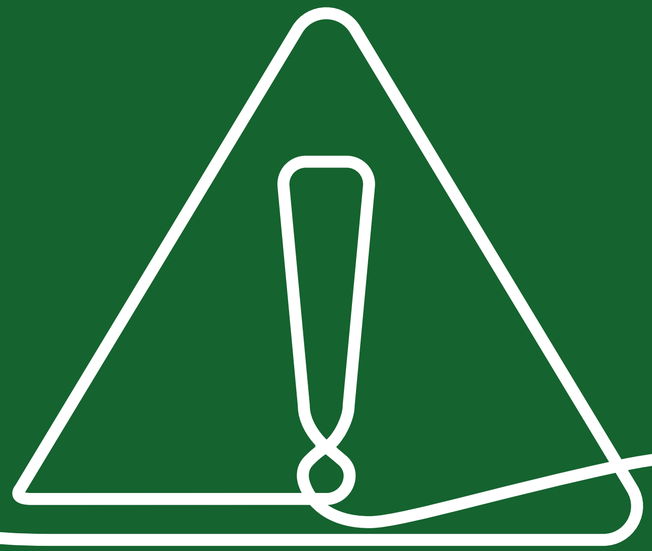
Managed.sa

Cybersecurity Orchestrator



Risk

Management Services

Risk Assessment and Analysis

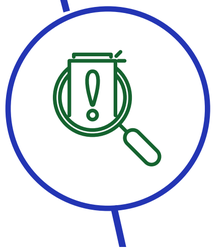
Risk Management Framework Implementation

Managed.sa
Cybersecurity Orchestrator

Risk Assessment and Analysis

A cybersecurity risk assessment is a systematic process aimed at identifying vulnerabilities and threats within an organization's IT environment, assessing the likelihood of a security event, and determining the potential impact of such occurrences.

Managed.sa
Cybersecurity Orchestrator



What?

A cybersecurity risk assessment is a systematic process aimed at identifying vulnerabilities and threats within an organization's IT environment, assessing the likelihood of a security event, and determining the potential impact of such occurrences.

Why?

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 to ensure the resilience of IT systems.

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

Who?

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.

Risk Management Framework

Implementation

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 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 and international risk assessment framework is the ISO 27001:2022. This standard provides a comprehensive approach to information security management, including requirements for risk assessment and risk treatment.

managed.sa can also develop the customized risk assessment frameworks and methodologies for your organizations. Whatever approach an organization chooses, the goal should be to identify, assess, and prioritize risks to information and information systems.

Managed.sa
Cybersecurity Orchestrator

How to implement Risk Management Framework?

There is no one-size-fits-all approach to implementing the Risk Management Framework. Organizations should tailor their implementation plans to their specific needs and resources.

However, there are some general steps that all organizations should take when implementing the Risk Management Framework:

1. **Assess your organization's current cybersecurity posture**
   What are your current cybersecurity capabilities and practices? What gaps exist in your cybersecurity defenses?

2. **Identify which aspects of the Risk Management Framework are most relevant to your organization**
   Not all parts of the framework will be equally important for all organizations. Focus on the parts of the framework that will have the biggest impact on your organization's cybersecurity posture.

3. **Develop a plan for implementing the Risk Management Framework**
   This plan should include a timeline, a budget, and the resources needed.

4. **Implement the Risk Management Framework**
   This will involve putting the plan into action and making changes to your organization's cybersecurity practices.

5. **Evaluate the effectiveness of your implementation**
   As your organization's cybersecurity needs change over time, so too should your implementation of the framework.

Managed.sa
Cybersecurity Orchestrator

3273 Anas Ibn Malik - Al Sahafah Dist.
Riyadh 13321 - 8347
Kingdom of Saudi Arabia

+966 11 4185222

managed.sa