CompTIA

RISK MANAGEMENT: FREE RESOURCES TO DOWNLOAD

BUILDING AND IMPLEMENTING AN IT RISK MANAGEMENT PLAN IS CRITICAL IN TODAY'S DIGITAL-DRIVEN WORLD.

CompTIA

Common Risk Management Frameworks

There are numerous risk management frameworks that exist today. It's important to understand that such frameworks represent only the beginning of the GRC maturity process. As you begin improving organizational processes, it can be useful to consult appropriate frameworks, such as those listed below.

Framework	Description
NIST Risk Management Framework (RMF)	Provides a U.S. government-defined process meant to integrate security, privacy and cyber supply chain risk management. The goal is to create a systematic approach that resembles a system development lifecycle. This framework has been adopted worldwide.
ISO 27001 & ISO 27002	These two documents enable organizations of any kind to use security controls to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties. ISO 27001 provides information about industry-accepted security controls. The ISO 27002 document is a supplement that explains best practice suggestions and guidance for implementing the security controls found in ISO 27001.
NIST 800-53	This particular document is aimed at recommending specific security and privacy controls for U.S. federal government agencies. While it does not officially specify controls for national security organizations, it nevertheless is a common resource for both public and private organizations.
NIST 800-171	Originally meant as a companion to NIST 800-53, the 800-171 document is meant to provide organizations, including U.S. federal agencies, with information about how to control unclassified information. Many organizations around the world have adopted this document as a baseline framework for managing risk.

CompTIA

How to Build and Implement a Risk Management Plan

Building and implementing an IT risk management plan, or a more resilient risk management plan, is critical in today's digital-driven world. The key goal for building a risk management plan is to write, develop and practice the plan. Practical and realistic risk management needs to be written and documented, or it will remain only an idea and set of abstract strategies. Here are 4 steps to build and implement a practical risk management plan that focuses on maturing processes.

1

Identify Your Organizational Risk and Potential Vulnerabilities

What does risk look like for your organization?
What common risks does your organization face?
What are your potential vulnerabilities?
What data needs to be protected most?
What is the weakest point of your business infrastructure?

2

Evaluate and Assess Risk to Focus on More Zero Trust Activities vs. "Good to Go"

What practices and processes can help evaluate and mitigate risk?
Do you follow a zero trust framework?
What checks and balances are in place to mitigate internal and external risk?

3

Ensure Effective Communication Between the IT and Business Leadership Teams

Who are the key players in risk management?
Does everyone know their role in protecting the organization?
Are you speaking a common language? Does everyone understand the terminology?
Do you have regular meetings/touchpoints to proactively evaluate risk?

4

Review and Run Risk Scenario Simulations and Exercises

What activities should be included in a tabletop exercise?
Who should participate?
What other simulations or exercises should the organization practice?
How often should simulations and exercises occur?

CompTIA

Best Practices for Effectively Managing Information Risk in IT

The primary best practice for organizations to effectively manage information risk in IT is to focus on maturing security processes within your organization. The best practices for practical risk management focus on the processes versus the compliance or GRC demands of the organization. For better risk management, organizations need to shift the risk mindset from avoidance or tolerance to implementing more zero trust within their processes.

Engage with upper management

- Conduct regular meetings with organizational leaders to understand their needs and gain consensus and buy-in
- Gather data and identify commonalities to make informed decisions
- Communicate using a common language to apply security controls and make appropriate changes

Identify business processes that need modification

- Conduct a series of root-cause investigations to identify processes that cause issues
- Look at the overall behavior organization before undergoing a technical investigation

Determine existing technical procedures and controls through vulnerability assessment and penetration testing

- Conduct a business impact analysis
- Identify risk management strategies that apply to your particular organization, such as acceptance, avoidance, transference, cybersecurity insurance and mitigation
- Identify impacts on business processes
- Determine how issues can impact an organization in terms of laws and privacy frameworks that apply to the organization

Codify changes

- Work with management and technical teams to create and implement changes that will help mature security

CompTIA