Risk Management - The NIST RMF

Objectives:

At the end of this episode, I will be able to:

Understand what the NIST Risk Management Framework is.

Explain the importance of the NIST Risk Management Framework for an organization that wants to manage risk.

Identify the phases of the NIST Risk Management Framework.

Define what key action(s) should be taken in each phase of the NIST Risk Management Framework.

External Resources:

Risk Management - The Basics

What is the NIST Risk Management Framework (RMF)? -

A structured and continuous process that integrates information security and risk management activities into the system development life cycle (SDLC).

It follows a security life cycle, which involves six stages:

```
▪ Categorization of the Information System - the initial stage, which involves
defining criticality or sensitivity of the information system according to the
potential worst-case scenario. This shows the adverse impact to the mission or
the business.

▪ Selection of the Security Controls - Categorize the information system, and
then select the baseline security controls under a NIST risk management
framework. Apply tailored guidance and supplemental controls (if needed) based
on risk assessment.

▪ Implement the Security Controls - Implement security controls within the
enterprise architecture using sound system-engineering practices. Apply
security configuration settings.

▪ Assess the Security Controls - Determine security control effectiveness by
ensuring correct and effective implementation of the controls as per required
operation and compliance with security requirements for the information system.

▪ Authorize the Information System - Determine risk to organizational
operations and assets, individuals, other organizations, and the nation; if
acceptable, authorize the operation.

▪ Monitor Security State - Continuously track changes to the information
system that may affect security controls, and reassess control effectiveness.
```