What is NIST 800-30?

- NIST 800-30 acts as a bridge to help both parties understand what it will take to bolster their organizational and computer security defences against inside and outside threats.

- NIST SP 800 gives risk assessment teams clear guidance on analysing and reporting risks to company leaders.

- Using a standard language format makes it easier to translate the impacts to the company in a business format, including the type of threats faced by an organization, how they could impact the company, and potential financial losses.

How NIST 800-30 fits into cybersecurity risk management

The NIST 800-30 framework guides company leaders and security personnel in creating and executing risk assessments that follow the NIST framework. Organizations should conduct risk assessments to gain a better understanding of the following:

- Any internal and external vulnerabilities that currently exist
- The most relevant threats to the company
- How various threats would impact business
- The likelihood of a threat occurring

How to implement NIST 800-30 in your organization

1) Prepare for a risk assessment

2) Conduct risk assessment

3) Communicate results of the risk assessment

4) Maintain risk assessment

1) Prepare for a risk assessment

- Determining the scope of the risk assessment
- Coming up with assumptions and identifying restraints associated with the assessment
- Identifying the information sources to use for the risk assessment

- Determining which analytical approaches and models to use during the risk assessment

2) Conduct risk assessment

- The data held by your organization
- Where you hold the information (IT systems)
- What technology infrastructure your company has in place
- The value of the information you're looking to protect

IDENTIFY SOURCES OF THREAT
PINPOINT VULNERABILITIES AND PREDISPOSING CONDITIONS
DETERMINE THE LIKELIHOOD OF OCCURRENCE

DETERMINE THE MAGNITUDE OF THE IMPACT: Examine the extent of harm a threat could cause to your operations, assets, workers, or vendors.

- Data repositories
- Information systems
- Business applications
- Communication links

3) Communicate results of the risk assessment

Decision-makers should have risk assessment information to guide their decisions around security investments. Formats to use include interactive dashboards, briefings, or risk assessment reports. one can make the presentation formal or informal based on your company environment.

4) Maintain risk assessment

Organizations need to keep the information within risk assessments current to support ongoing decision-making related to risk response.

A change management mechanism should be in place to capture changes found through risk monitoring.

NIST 800-53 control families

Access control

The access control section covers any controls tied to system, network, and device access. The guidance helps organizations correctly implement the following:

- Access control policies

- Account management policies
- User privileges

Awareness and training

Audit and accountability

This control family provides explanations on establishing event logging and audit procedures, including the following:

- Baselines for audit records
- How much capacity to allot for log storing
- How to conduct reviews and log monitoring

Assessment, authorization, and monitoring

focus is on improving security and privacy controls. You can also learn about delegating responsibilities, setting up assessment plans, and locating and fixing vulnerabilities.

Configuration management

The goal is to help organizations lower their risk of someone installing unauthorized hardware or software within business systems. It contains details on the following:

- Baseline system configurations
- Configuration policy
- Dealing with managed access to devices

Contingency planning

The guidance here teaches companies about controls needed to prepare for potential breaches or system failures. It details system backup and alternative storage options to mitigate potential system downtime.

Identification and authentication

This section covers controls to identify users and devices using a company’s systems and networks. You can use the information here to strengthen your management policies and lower risks associated with unauthorized access.

Incident response

The IR family covers enhanced controls used to cover specific threat events like data breaches, supply chain issues, malicious code, and dealing with PR fallout.

Maintenance

This section covers various methods of conducting system maintenance, inspections, software updates, and logging. It outlines specific policies aimed at reducing risks associated with outages. You can also learn more about managing maintenance personnel.

Media protection

The media protection control family offers insight into storing, using, and destroying company media files safely. Use it to come up with baseline controls for your organization and how to lower your organization's risk of experiencing a data breach.

Physical and environmental protection

The controls outlined in this section cover physical facility and device access. Use the techniques outlined here to establish physical access control policies. You can also use them for planning responses to sudden power loss or the need to relocate to a different facility in an emergency.

Planning

The controls in the planning section cover baseline system settings for security controls related to:

- System architecture
- System security plans
- Privacy security plans
- Management processes

Personnel security

- This control family covers procedures related to personnel management and provides insight into IT security risks linked to different company positions. Use them to establish organizational guidelines around terminating contract