UNIT 6

Developing a Cyber Security & Risk Management Plan

Learning Outcomes
By the end of this unit the learner will be able to:
✓ Understand the functions and objectives of risk management ✓ Contribute to the development of an effective risk management plan ✓ Identify and classify cyber assets in an organizational setting

Unit 6

Developing a Cyber Security & Risk Management Plan

Effective information systems are critical to the success of any organisation. Secure management of intellectual property and confidential or sensitive information provides competitive advantage and helps protect corporate reputation. This is true whether that information is in the form of a product design, a manufacturing process, a negotiating strategy or sensitive personal data. At the same time, the need to access and share information more widely, using a broad range of connecting technologies, increases the risk of that information becoming compromised or misappropriated.

No usable system is 100 percent secure or impenetrable. The goal of a risk management program is to identify the risks, understand their likelihood and impact on the business, and then put in place security controls that mitigate the risks to a level acceptable to the organization. In addition to assessment and mitigation, a robust risk management program includes ongoing evaluation and assessment of cyber security risks and controls throughout the life cycle of smart grid component software.
The following checklist summarizes security best practices and controls that you should consider implementing. This section includes details about the practices.

	Activity / Security Control	Rationale
	Provide active executive sponsorship.	Active and visible support from executive management at each stage of planning, deploying, and monitoring security efforts is crucial to success.
	Assign responsibility for security risk management to a senior manager.	Have security risk mitigation, resource-allocation decisions, and policy enforcement roll up to a clearly defined executive with the requisite authority.
	Define the system.	Careful system definitions are essential to the accuracy of vulnerability and risk assessments and to the selection of controls that will provide adequate assurances of cyber security.

	Identify and classify critical cyber assets.	It is important to understand the assets that may need to be protected, along with their classification (e.g., confidential information, private information, etc.). That way an informed decision can be made as to the controls needed to protect these assets, commensurate with risk severity and impact to the business.
	Identify and analyze the electronic security perimeter(s) (ESPs).	To build a threat model, it is important to understand the entry points that an adversary may use to go after the assets of an organization. The threat model then becomes an important component of the risk assessment.
	Perform a vulnerability assessment.	Realistic assessments of (a) weaknesses in existing security controls and (b) threats and their capabilities create the basis for estimating the likelihood of successful attacks. They also help to prioritize remedial actions.
	Assess risks to system information and assets.	The risk assessment combines the likelihood of a successful attack with its assessed potential impact on the organization's mission and goals. It helps ensure that mitigation efforts target the highest security risks and that the controls selected are appropriate and cost-effective for the organization.

Activity / Security Control	Rationale
Select security controls.	Appropriate management, operational, and technical controls cost-effectively strengthen defenses and lower risk levels. In addition to assessed risks, selection factors might include the organization's mission, environment, culture, and budget.
Monitor and assess the effectiveness of controls.	Effective testing and ongoing monitoring and evaluation can provide a level of confidence that security controls adequately mitigate perceived risks.

Establishing a Risk Management Framework

It is important for an organization to define a risk management framework that will be used to:

- Define the system.
- Identify cyber assets and their classification.
- Identify the electronic security perimeter (ESP) protecting these assets.
- Conduct vulnerability assessment:
- Identify threats.
- Identify vulnerabilities.
- Identify security risks along with their impact and likelihood.
- Assess the effectiveness of existing security controls in mitigating the risks.
- Recommend new security controls or changes to existing security controls to mitigate the severity of the risks to a level acceptable to the organization.
- Continuously monitor the effectiveness of security controls.
- Periodically repeat this process to account for system changes and changes in the threat landscape.

These steps are described in more detail below.

Defining the System

Careful system definitions are essential to the accuracy of vulnerability and risk assessments and to the selection of controls that will provide adequate assurances of cyber security. Not all systems require the same level of protection.

The following are a few major elements of a system definition:

- The logical and physical boundaries of the system within its environment:
- Which components and resources belong to the system?
- Which are external to the system?
- The system's mission and primary functions.
- The system's architecture (physical, logical, and security) and data flows.
- Details for interfaces and protocols.
- Types of information the system stores, uses, or transmits, and the sensitivity of each.
- Existing management, technical, operational, and physical security controls.

Cyber Asset Identification and Classification

Systems have access to and operate using assets that adversaries may want to compromise. Using a risk-based methodology to identify critical cyber assets is a crucial step in managing security risk. Below find important definitions:

- **Critical assets:** Facilities, systems, and equipment that if destroyed, degraded, or otherwise rendered unavailable would affect the reliability or operability of the bulk electric system.
- **Cyber assets:** Programmable electronic devices and communications networks including hardware, software, and data.
- **Critical cyber assets:** Cyber assets essential to the reliable operation of critical assets.

Note: Risk assessments generally consider both the impact of an adverse event and the likelihood that the event will occur. However, the identification of critical assets considers only the impact of the event; it assumes that the loss will in fact occur.

Identifying Critical Cyber Assets

Guidelines for identifying critical assets

The following steps summarize the process:

1. Identify critical assets.
   - Identify the asset types to be evaluated:
     - Facilities such as generation resources, transmission substations, control centers.
     - Special systems, real-time decision-support systems.
   - Enumerate the assets within each type. This is the list of critical assets.
   - List the essential functions of each critical asset.

2. Identify cyber assets associated with a critical asset. Grouping cyber assets by application can simplify the process.
3. Narrow the list of identified cyber assets from step 2 to those supporting the essential functions of critical assets.

A designated senior manager or delegate must annually review and approve the lists of critical assets and critical cyber assets.

Classifying Cyber Assets

Classifying cyber assets as public, restricted, confidential, or private will help dictate the rigor with which they need to be protected by security controls.

Consider classifying your cyber assets in the following categories:

Public

This information is in the public domain and does not require any special protection. For instance, the address and phone number of the headquarters of your electric cooperative is likely to be public information.

Restricted

This information is generally restricted to all or only some employees in your organization, and its release has the potential of having negative consequences on your organization's business mission or security posture. Examples of this information may include:

- Operational procedures
- Network topology or similar diagrams
- Equipment layouts of critical cyber assets
- Floor plans of computing centers that contain critical cyber assets

Confidential

Disclosure of this information carries a strong possibility of undermining your organization's business mission or security posture. Examples of this information may include:

- Security configuration information
- Authentication and authorization information
- Private encryption keys
- Disaster recovery plans
- Incident response plans

Personally Identifying Information (PII)

PII is a subset of confidential information that uniquely identifies the private information of a person. This information may include a combination of the person's name and social security number, person's name and credit card number, and so on. PII can identify or locate a living person. Such data has the potential to harm the person if it is lost or inappropriately disclosed. It is essential to safeguard PII against loss, unauthorized destruction, or unauthorized access.

Identifying the Electronic Security Perimeter (ESP) Protecting Cyber Assets

All critical cyber assets should reside behind logical security protections. Each collection of logical security protections is an electronic security perimeter (ESP).
This logical border is the collection of proxies, gateways, routers, firewalls, encrypted tunnels, etc., that monitor and control communications at the external boundary of the system to prevent and detect malicious and other unauthorized communication. At a minimum, identify and document the following:

- The critical cyber assets requiring an ESP.
- The access points to each perimeter, for example:
  - ✓ Firewalls
  - ✓ Routers
  - ✓ Modems
  - ✓ Virtual private network (VPN) endpoints
  - ✓ Proxy servers
  - ✓ Web servers

The analysis of ESPs, and whether critical cyber assets reside fully within a secure perimeter, requires care. Identifying all access points and the controls on them can be tricky, and it is possible to overlook an avenue of access that could be exploited.

Conducting a Vulnerability Assessment

Perform a cyber-vulnerability assessment of the access points to each ESP at least once a year. The vulnerability assessment should examine ways in which the security perimeter can be breached and existing security controls bypassed to compromise confidentiality, integrity, or availability of critical cyber assets.

A cyber threat is any entity or circumstance that has the potential to harm an information system and, through that system, the organization's mission and goals. A cyber vulnerability is a gap or weakness in a system's security controls that a threat can exploit.

Vulnerability assessments broaden and deepen awareness of threats, attacks, vulnerabilities, and the effectiveness of existing controls. They also establish baselines that future assessments can use to determine whether planned improvements have occurred.

Assessing and Mitigating Risks

Vulnerability assessments will identify certain risks. An important part of the risk management process is to determine the severity of each risk as a function of its impact and likelihood. It is also important to understand the extent to which existing security controls completely or partially mitigate each risk. It is then possible to enumerate the gaps in protection and make an informed risk-based decision on next steps.

Although a risk management strategy strives for risk prevention where practical, it also must balance the costs and benefits of security controls. The goal is cost-effective controls that ensure acceptable risk levels for participating cooperatives and the smart grid as a whole. We can think of security risks as belonging to one of three main categories:

- People and policy
- Process
- Technology

A cyber security program must be comprehensive—it is only as strong as its weakest link. Failure to develop appropriate controls in any category provides openings for attackers. This guide includes sections that describe common risks and mitigations in each category.

Assessing Impact and Risk Levels

A careful risk assessment considers both the likelihood of a successful attack and its impact on the organization's mission and goals. Impacts could be ranked as follows:

- **Safety:** Causing risk to life and limb.
- **Outage:** Leading to improper operation of a power system device, possibly resulting in a consumer outage.
- **Privacy:** Disclosing private data, such as social security or credit card numbers.
- **Monetary:** Leading to increased tangible costs to the utility.

Once your organization identifies and prioritizes risks and the gaps that exist in current security controls, it is possible to build a prioritized remediation plan that focuses on improving existing security controls or adding security controls to mitigate high-priority risks first, then medium priority, and then low priority (as appropriate).

Mitigating Risks with Security Controls

Understanding an event's impact allows the organization to make informed decisions about mitigating the risk by some combination of the following:

- Reducing the likelihood of its occurrence
- Detecting an occurrence
- Improving the ability to recover from an occurrence
- Transferring the risk to another entity (e.g., buying insurance)

It is important to apply risk mitigation strategies at each stage in the life cycles of system components and protocols. Questions such as the following can help guide strategy choices:

- Is the risk a compliance issue, a privacy issue, a technical issue, or some other issue?
- Does the mitigation deal primarily with people, process, or technology?
- Is the assessed risk acceptable to the organization?
- Is the cost of fully remediating the risk reasonable?

The following steps summarize a process for assessing and mitigating risks:

1. **System characterization:** Identify the system's boundaries, resources, and information.
2. **Threat identification:** List all entities (natural, human, or environmental) that could harm the system's capability to fulfill its critical functions. List their potential attack methods and assess their capacity and motivation (for humans) to mount an attack.
3. **Vulnerability identification:** List and assess all gaps or weaknesses in the system's management, operational, and technical security controls that a threat could accidentally or intentionally exploit to harm the system.
4. **Risk assessment:** Estimate the risks to the system posed by specific threats and vulnerabilities. This process consists of four tightly linked activities:
   - Analyze the capability of existing security controls to prevent an occurrence of the adverse event, detect an occurrence, and contain the impact of an occurrence.
   - Estimate the likelihood (high, medium, low)11 of an occurrence given the nature of the vulnerability, the capability of existing threats, and the strength of current controls.
   - Analyze the potential damage an occurrence would do to the system, its data, and the organization's business goals. Rate the potential impact as high, medium, or low.
   - Derive the risk rating from the combination of likelihood and impact.
5. Control recommendations: Identify and select additional security controls to eliminate the risks or lower them to an acceptable risk level.

Evaluating and Monitoring Control Effectiveness

Analysis can show the absence or presence of controls, but testing is usually required to demonstrate the effectiveness of each control in mitigating a particular risk. The organization must develop, implement, and maintain cyber security test procedures and tools. Multiple types of testing may be required:

- Testing of personnel awareness and capability requires tailored skills reviews.
- Testing of security features and software logic requires manual penetration testing.
- Testing of software security requires static analysis tools.
- Testing of Web applications requires dynamic testing tools.
- Testing of protocols requires interoperability harnesses and fuzzing tools.
- Testing of hosts and networks requires network penetration testing tools.

Notes:

- Ensure that skilled individuals perform security testing and analysis with tools.
- The level of detail in test plans depends on the type of testing. It can range from simple plans for basic testing to detailed plans for complex interoperability and security testing.
- Testing must reflect production environments, and the results must be documented.