

Cybersecurity Law and Policy

Prepared by Dr. Kamal Alieyan

Lecture 7



Lecture 7

Prepared by
Dr. Kamal Alieyan

Lecture Objective



- To understand the concept of cyber risks.
- To analyzing risks, assessing risks, and managing risks, and how are they significant for ensuring security in organizations and cyberspace.
- To understand risk remediation, and some use cases involving cyber risks.

Lecture topics



- **7.1 INTRODUCTION TO CYBER RISKS**
- **7.2 CYBER ATTACKS AND THEIR BUSINESS SIGNIFICANCE**
- **7.3 KEY CYBER RISKS AND THREATS**
- **7.4 WHO SHOULD OWN CYBERSECURITY RISK?**
- **7.5 CYBERSECURITY RISK IDENTIFICATION AND MANAGEMENT**
- **7.6 RISK IDENTIFICATION USING SWOT ANALYSIS**
- **7.7 RISK ANALYSIS**
- **7.8 RISK ASSESSMENT**
- **7.9 RISK ASSESSMENT FRAMEWORKS**
- **7.10 RISK MANAGEMENT**
- **7.11 RISK MANAGEMENT FRAMEWORK**
- **7.12 RISK REMEDIATION**

Chapter

07

7.1 INTRODUCTION TO CYBER RISKS

- The **cyber risk** defined as any risk that may result due to financial losses, any kind of disruption, or damage to the reputation of an organization.
- This often leads to the failure of an organization's information technology (IT) systems.
- **Cyber risk could materialize in a variety of ways.**
- Some of these ways are listed as follows:
 - Deliberately breaching security to gain access to information systems
 - Unauthorized access to information
 - Unintentional breaches of security
 - Accidental breaches of security
 - Poor system integrity promoting operational IT risks
 - Unsatisfactory management of cyber risks that may support an assortment of cybercrimes.

Chapter

07

7.1 INTRODUCTION TO CYBER RISKS

- It is a well-known fact that businesses commonly find themselves in the middle of unpleasant situations when they struggle to recover lost assets in order to prevent theft in the future.
- Regardless of whether a business is big or small, cybercrime could be lurking just around the corner.
- Recently, more and more small businesses are being targeted by cybercriminals, therefore, without the right preventative measures in place, it could aggravate even further.
- Hence it is necessary to get more familiar with the cyber risks that organizations may face.
- It is often seen that the more sophisticated and extensive a business digital operations are, the greater the chances of cyber risks being involved.

7.1 INTRODUCTION TO CYBER RISKS

- The following are some elements that contribute to elevation of cyber risks:
 - Employees or customers accessing the organizational systems from remote locations.
 - Staff making utilization of organization-owned devices at their homes or while traveling.
 - Employee access to administrative privileges on the organization's network or computers.
 - A policy emphasizing on the use of bring your own device (BYOD) in the workplace.
 - Accessing public buildings without authorization.
 - Employees using computers for accessing bank accounts or initiating monetary transactions.
 - Employees neglecting certain policies regarding regular updating of passwords.
 - Critical information that may be lost as a result of a network disaster.
 - Neglecting to review the company's cybersecurity policies from time to time.

7.1 INTRODUCTION TO CYBER RISKS

- All businesses come across the risks of cyber breaches at some point during their life cycle.
- However, understanding the level of risks, the factors that led to the risks, and the origin of threats, i.e., source of the threats may be significantly effective in preparing a productive response.
- With organizations becoming more and more technology and business driven, they become more prone to attacks and threats.
- This is a direct result of the expanding dependence on networks, systems, programs, social media, and information globally.
- This in turn makes data breaches an increasingly common affair in cyberspace.
- Cyber-attacks may have a negative business sway, and these frequently emerge from deficiently secured information.

Chapter

07

7.1 INTRODUCTION TO CYBER RISKS

- Global connectivity and increased use of cloud services with poor default security parameters often lead to an increased risk of cyber-attacks outside the organization.
- IT risk management may effectively address how access control needs to be complemented by sophisticated cybersecurity professionals, software, and cybersecurity risk management.
- With sophisticated attacks, it may not be sufficient to bank upon traditional IT professionals and security controls for information security.
- There is an urgent need for sophisticated threat intelligence tools and security programs that may assist in reducing an organization's cyber risk and potential attack surfaces.
- Decision-makers in the organizations must take into account assessments when dealing with third-party vendors.
- There is likewise a need to present risk mitigation techniques and cyber incident response (IR) plans in associations for when a breach may take place.
- Figure 6.1 is a manifestation of how cyber risks may be initiated.

7.1 INTRODUCTION TO CYBER RISKS

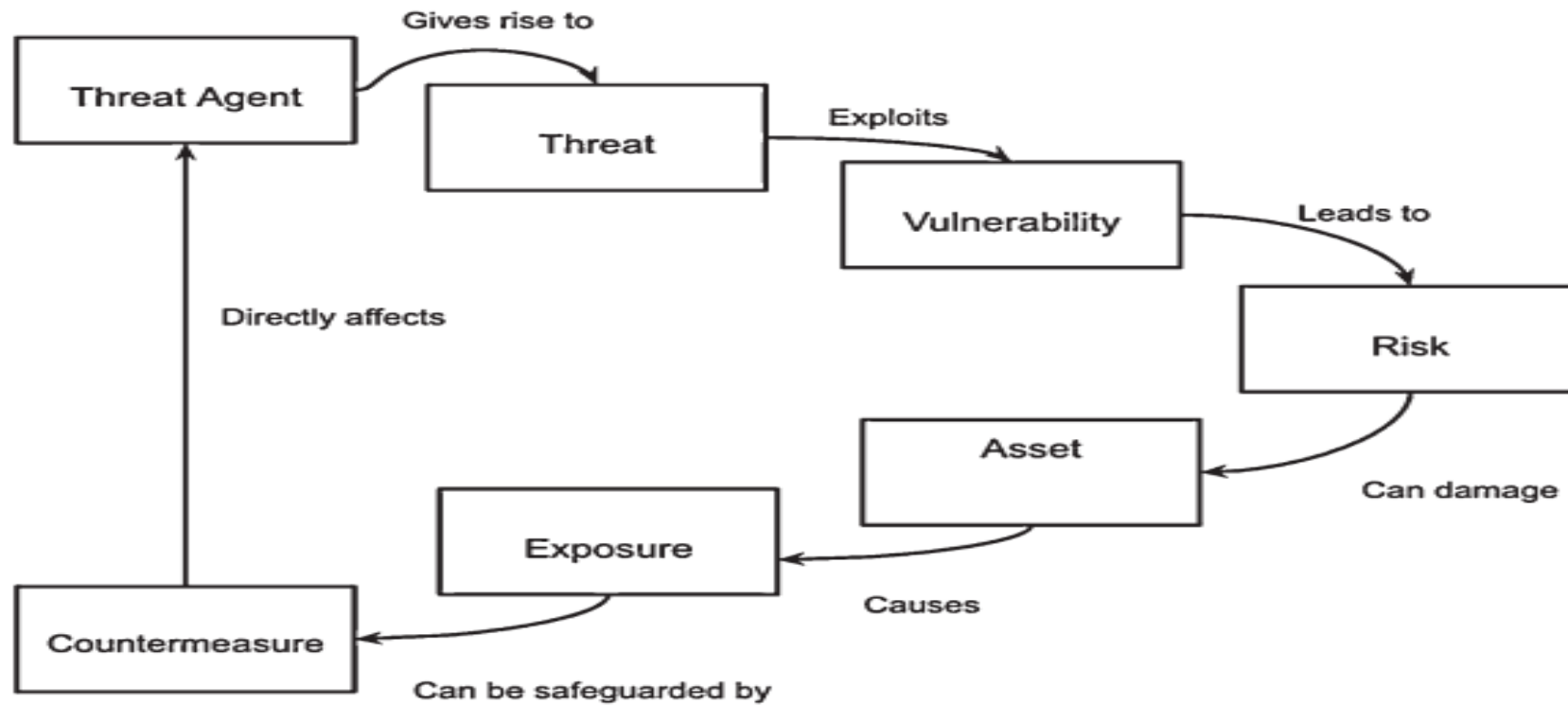


FIGURE 6.1 Understanding cyber risks.

Chapter

07

7.1 INTRODUCTION TO CYBER RISKS

- Threat Agent might be characterized as an individual or group that can exhibit a threat.
- It is necessary to **determine** who could exploit the assets of an organization and how they might use them against the organization. Therefore, a threat agent may also be thought of as a technique utilized in penetrating the security of an office, operation, or framework by abusing a weakness.
- **Cyber threats** are cybersecurity circumstances or events that are capable of causing harm by way of their outcome.
- A very common threat is a social-engineering or phishing attack.
- Cybersecurity threats are actualized by threat actors. These threat actors may be individuals or entities who have the potential to initiate a threat.
- Although natural disasters, and other environmental and political events, may often constitute threats, they are not considered threat actors.

Chapter

07

7.1 INTRODUCTION TO CYBER RISKS

- Some **basic threat actors** are monetarily propelled lawbreakers (cybercriminals), politically spurred activists, nation-states and competitors.
- In an office environment, careless employees and disgruntled employees are threat actors.
- Vulnerabilities consider as a weaknesses in a system that have the potential to make threat results conceivable and are possibly significantly riskier.
- A single vulnerability is enough to exploit a system. Consider a simple structured query language (SQL) Injection attack that could give an assailant full command over delicate information.
- Instances of basic vulnerability are SQL injection, Cross-site Scripting, server misconfigurations, delicate information communicated in plaintext, and that is just the beginning.
- Ordinarily, risks are mistaken for threats despite the fact that there is a slight contrast between them.

Chapter

07

7.1 INTRODUCTION TO CYBER RISKS

- A **cybersecurity risk** may be a combination of a threat probability and loss/impact.
- This loss impact is usually in the financial terms, however, evaluating a breach is not easy.
- Essentially, this translates to the following:

$$\text{Risk} = \text{Threat Probability} \times \text{Potential Loss}$$

- The situation of risk must be avoided due to the losses that result from that scenario.
- Let us consider a hypothetical example showing that the risk construction is a given scenario.
- A very common vulnerability is **SQL Injection**, which enables data theft, which is a significant threat.
- Attackers who are motivated financially could serve as **threat actors** here.
- Also, the loss of sensitive data will not only impact the organization in monetary terms, but will also affect its reputation.

Chapter

07

7.1 INTRODUCTION TO CYBER RISKS

- This may be effective in the prevention and mitigation of security breaches.
- Effective risk assessment and risk management rely on good understanding. It takes into account designing efficient security solutions based on threat intelligence, and may also be responsible for building a viable security strategy and a cybersecurity system.
- Threat agents may be responsible for generating threats which often leads to vulnerabilities being exploited.
- Once vulnerabilities are exploited, it leads to cyber risk.
- Cyber risks have the capability to damage assets, and this may lead to exposure.
- This calls for safeguarding the system, which may be performed using countermeasures.

7.1 INTRODUCTION TO CYBER RISKS

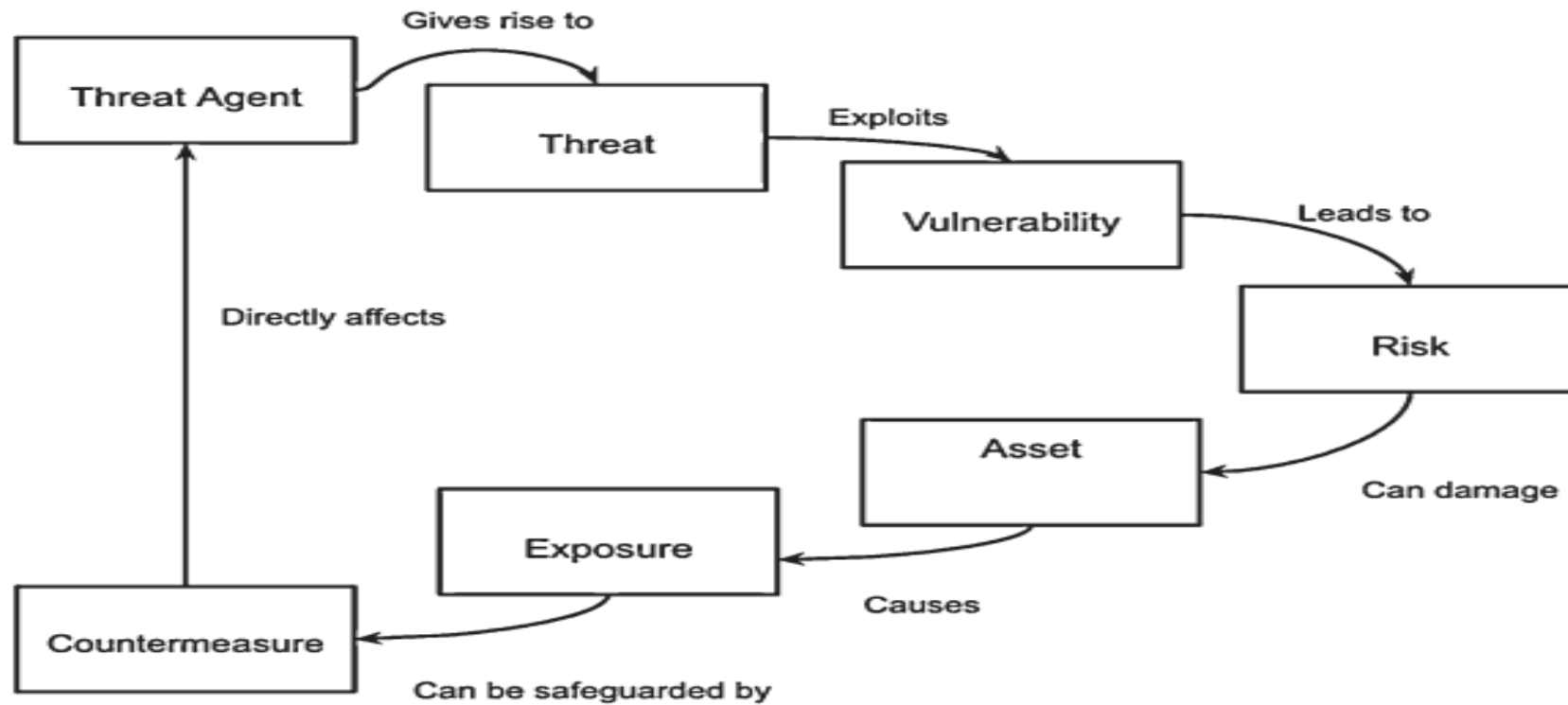


FIGURE 6.1 Understanding cyber risks.

7.2 CYBER ATTACKS AND THEIR BUSINESS SIGNIFICANCE

- Regardless of being helpful, numerous **IT arrangements** are lacking for giving cyber-attack assurance from complex attacks and poor configuration.
- With the uncontrolled multiplication of innovation and growth of technology, there is more unapproved access to the organization than ever before.
- There is a tremendous increase in information provided to third parties by means of supply chains, customers, and other providers.
- With organizations increasingly storing, organizations are progressively storing enormous volumes of personally identifiable information (PII). For this, they are depending on external cloud providers that should be designed accurately so as to adequately secure information.
- This leads to added risk; additionally, there is an increase in the number of devices that are always connected in data exchange.

7.2 CYBER ATTACKS AND THEIR BUSINESS SIGNIFICANCE

- With organizations globalizing and the web of employees, customers, and third-party vendors increasing, there is also an increase in expectations of instant access to information.
- Consumers expect instant real-time access to data from anywhere. The consequence is an exponential increment in the attack surface for malware, weaknesses, and every other exploit.
- Unexpected cyber threats may emerge from threatening unfamiliar powers, contenders, organized hackers, insiders, poor configuration, and third-party vendors.
- This makes organizations rely on software that may not only assist their third-party vendors but can also continuously monitor for data breaches. The need of recognizing, tending to, and conveying a potential breach is more noteworthy than the preventive estimation of customary, repetitive IT security controls.
- Data breaches have a massive, negative business impact. This is because of the insufficiently protected data.

7.2 CYBER ATTACKS AND THEIR BUSINESS SIGNIFICANCE

- A **good risk management strategy** is external monitoring of risks through third and 4th-party vendor risk assessments. But, there is also a need for a comprehensive IT security management, without which an organization is prone to financial, legal, and reputational risk.
- Cybercrimes are additionally known to target businesses.
- Emerging new technologies based on IoT give rise to some of the biggest cyber threats.
- As the network keeps on expanding and more devices are added to the network for developing greater connectivity, cyber risks also increase. Thus security measures need to evolve, too.
- Some common reasons **why businesses fall victim to cyber-attacks** are as follows:
 - Staff shortcomings may make an organization vulnerable.
 - Cloud computing provokes security.
 - Ransomware can infiltrate networks.

7.3 KEY CYBER RISKS AND THREATS

- Cybersecurity is applicable to all systems that contribute to an organizations business operations and objectives. Also applied to an organizations compliance with regulations and laws.
- Organizations plans and actualize cybersecurity controls for ensuring the integrity, confidentiality, and availability of information assets.
- Cyberattacks, they may be committed as financial frauds, data theft, activist causes, and upset basic infrastructure.
- The common **sources of cyber threats** are as follows:
 - Nation-states
 - Cybercriminals
 - Hacktivists
 - Insiders
 - Service providers
 - Developers of substandard products and services

7.3 KEY CYBER RISKS AND THREATS

- To understand the **cyber risk profile of an organization**, it is necessary to identify the kind of information that would be valuable to outsiders. Hackers target data that can cause critical disturbance.
- It is important to know the data has the capability of causing monetary or reputational harm to the organization if it somehow happened to be obtained or made open.
- One such information is **PII** that includes names, social security numbers, and biometric records.
- The following may be considered as **potential targets to cybercriminals**:
 - Customer data
 - Employee data
 - Intellectual property (IP)
 - Product quality and safety
 - Contract terms and pricing
 - Strategic planning
 - Financial data

7.4 WHO SHOULD OWN CYBERSECURITY RISK?

- Cybersecurity risk management is usually set by leadership which may incorporate an organization's board of directors in the planning processes.
- Most organizations will also include a **Chief Information Security Officer (CISO).**
- The CISO establishes and maintains the enterprise vision.
- The CISO plans the strategies and programs to ensure that the information assets and customer data may be adequately protected.
- Some common **cyber defense operations** that are **undertaken by a CISO** are as follows:
 - Administering security procedures
 - Training and testing
 - Maintaining secure device configurations
 - Up-to-date software
 - Vulnerability patches
 - Deploying intrusion detection systems and establishing penetration testing
 - Configuring secure networks to manage and protect business networks

7.4 WHO SHOULD OWN CYBERSECURITY RISK?

- Deploying programs that may be useful for data protection and loss prevention
 - Deploying programs that will perform system monitoring for risks
 - Restricting access to least required privilege for employees
 - Encrypting data when required
 - Configuring cloud services
 - Implementing vulnerability management programs
 - Recruiting and retaining cybersecurity professionals
- It is significant for all degrees of an organization to comprehend its role in managing cyber risk.
 - Since vulnerabilities can come from any employee, it is fundamental to an organization's IT security to continually educate employees.
 - The employees must be educated on how to avoid common security pitfalls that may cause data breaches or other cyber incidents.
 - The National Institute of Standards and Technology's (NIST) cybersecurity framework (CSF) provides some of the best practices to manage cybersecurity risk.

7.5 CYBERSECURITY RISK IDENTIFICATION AND MANAGEMENT

- **Risk identification** the process of identifying and assessing threats to an organization, its operations, and its workforce.
- It takes into account assessing IT security threats.
- These threats may be in the form of malware and ransomware, accidents, natural disasters, and other potentially harmful events. The aim of such threats is to disrupt business operations.
- Hence it is important for companies to develop risk management plans.
- Companies that develop robust risk management plans conveniently minimize the impact of such threats, whenever they occur.

7.5 CYBERSECURITY RISK IDENTIFICATION AND MANAGEMENT

- The **process of risk identification and management** includes five core steps which are risk identification, risk analysis, risk evaluation, risk treatment, and risk monitoring.
1. **Risk Identification:** The primary objective of risk identification is to unveil what, where, when, why, and how something could affect an organization's ability to operate. For example, the possibility of wildfire may have an impact over a business located in central California. The consequences could be disruption in business operations.
 2. **Risk Analysis:** The procedure of risk analysis is utilized for researching the likelihood that a risk event may happen. Risk analysis additionally investigates the possible results of the related events. Considering the California wildfire example, it may be asserted that safety managers could be responsible for assessing how much rainfall has occurred over the past few months. This may give an idea with respect to the degree of harm the organization may confront if a similar situation takes place in the future.

7.5 CYBERSECURITY RISK IDENTIFICATION AND MANAGEMENT

3. **Risk Evaluation:** It is responsible for comparing the magnitude or intensity of each risk. It also ranks them according to prominence and consequence. Considering the same example, the effects of the wildfire could be weighed against the effects of a possible earthquake or landslide. Undergoing risk evaluation, the event that is identified to have a higher likelihood of occurring and causing harm, would rank higher.
4. **Risk Treatment:** Or risk response planning takes into account risk mitigation strategies, preventative care, and emergency courses of action which are made based on the surveyed estimation of each risk. Considering the wildfire example, risk managers may decide to house extra network servers offsite, so business activities could in any case continue if an onsite server is harmed. In addition, the risk manager may likewise create evacuation plans for employees.
5. **Risk Monitoring:** Risk monitoring is a constant procedure that adjusts and changes after some time. Repeating and continually monitoring the procedures can help guarantee maximum coverage of known and obscure risks.

7.5 CYBERSECURITY RISK IDENTIFICATION AND MANAGEMENT

- There are numerous ways to **identify risks**.
- Project managers (PM) often combine techniques to identify risks.
- Some of the **risk identification techniques** are as follows:

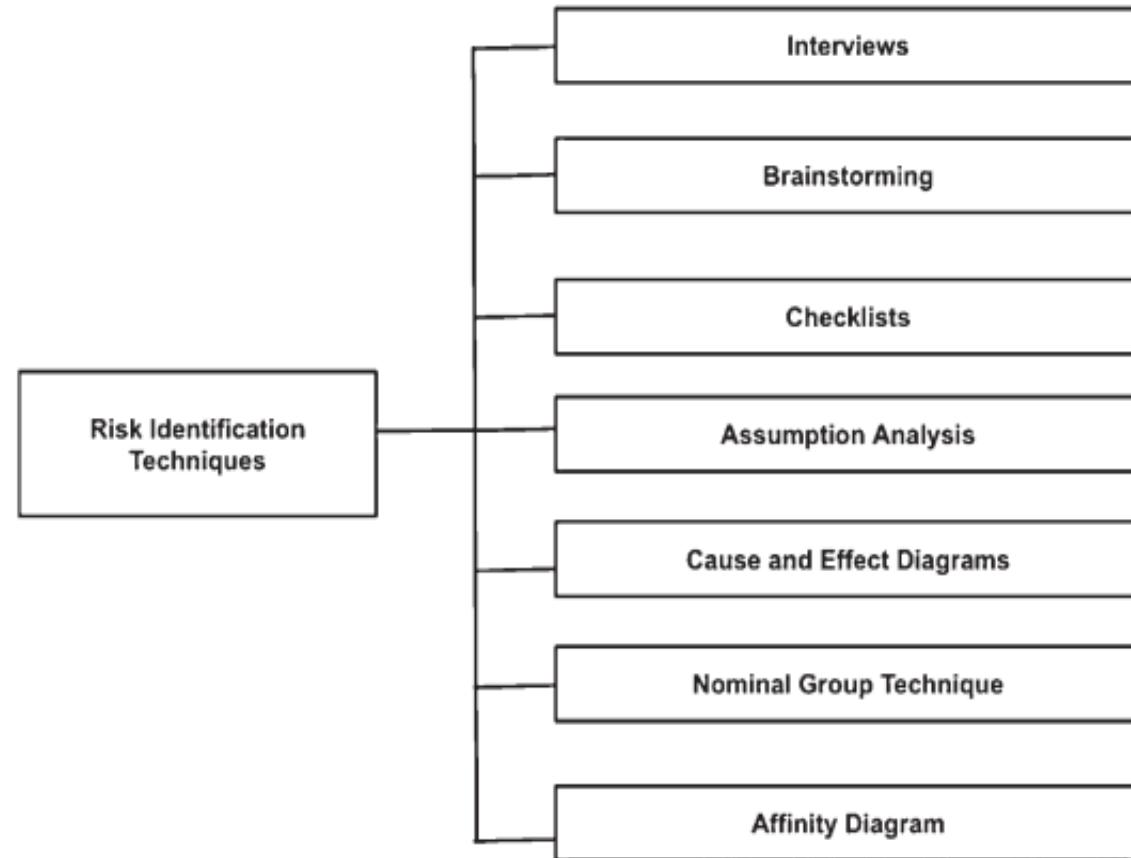


FIGURE 6.2 Risk identification techniques.

7.5 CYBERSECURITY RISK IDENTIFICATION AND MANAGEMENT

- An organization must identify the factors contributing to risks. The factors can be both internal as well as external.
- Risk identification can be performed in many different ways like:

1. Strategic Risk Identification:

This may be used to identify risks that arise from strategic choices made by an organization.

- Strategic risk identification must precede the finalization of strategic choices. This is to guarantee that potential risk issues are factored into the decision-making process for choosing the correct alternatives.
- Risks inherent to the chosen key decisions must be archived, surveyed, and overseen through the typical working of the arrangement of risk management.
- Strategic risks must be reviewed from time-to-time following changes in strategy, considering new and emerging risks.

7.5 CYBERSECURITY RISK IDENTIFICATION AND MANAGEMENT

2. Operational Risk Identification:

This is targeted to recognize risks inside the organizations functioning and operations:

- Operational risk identification is responsible for establishing vulnerabilities which are generally introduced by employees. Many times they are introduced by internal processes and systems, contractors, regulatory authorities and external events.
- Operational risk identification must be an embedded continuous process. This is because it is responsible for identifying new and emerging risks and considering shifts in the already existing risks through mechanisms like management and committee meetings, environmental scanning, process reviews.
- Operational risk identification must be repeated time and again, quarterly or yearly, especially when changes occur. This is helpful in recognizing new and rising risks.

7.5 CYBERSECURITY RISK IDENTIFICATION AND MANAGEMENT

3. Project Risk Identification:

It is responsible for identifying risks that are inherent to particular projects: project risks ought to be distinguished for every significant task, covering the entire lifecycle:

- Project risks must be identified for all major projects. They should cover the whole lifecycle of the project.
- In the case of long-term projects, reviewing must be performed at least once a year for identifying new and emerging risks.

7.5 CYBERSECURITY RISK IDENTIFICATION AND MANAGEMENT

- Before starting with the risk identification process, it is necessary to have knowledge of the business. For identifying risks that an organization may be prone to, there may be a need to learn from past experience as well as experiences of others. Only then can one come up with the best strategy for responding to the risks.
- The first thing to consider is the objectives of the institution, both implicit and explicit.
- Identifying emerging opportunities may also play an important role in risk identification.
- Although an organization will never be 100% risk free, it is necessary to establish controls.
- While working on the risk identification process, it is equally important to pay attention to identifying potential opportunities. Exploiting such opportunities may also improve an organization's performance.

7.5 CYBERSECURITY RISK IDENTIFICATION AND MANAGEMENT

- There are several steps to effectively identify risks in an organization. Some of these have been mentioned as follows:
 1. **Understanding What to Consider When Identifying Risks**
 2. **Gathering Information from Different Sources to Identify Risks**
 3. **Applying Risk Identification Tools and Techniques**
 4. **Documenting the Risks Identified**
 5. **Documenting the Risk Identification Process**

7.6 RISK IDENTIFICATION USING SWOT ANALYSIS

- **Risk Identification** has been characterized as a procedure of recognizing risks.
- Risks have the potential to prevent an institution, organization, or investment from achieving its goals. It incorporates documenting and communicating the concern.
- If a risk is **poorly identified**, it may not be possible for the project manager to properly and efficiently communicate the corresponding risk to team members as well as to other high-level stakeholders.
- **Poor identification of risks** makes it extremely difficult for the parties involved as well as stakeholders and partners to appreciate the measurement or force of the risk.
- As a consequence, instead of the risk materializing, the project manager and the team will be manifested ill-prepared.

7.6 RISK IDENTIFICATION USING SWOT ANALYSIS

- However, the issue in the first place is with the risk identification, since it was not understood or communicated properly
- **SWOT analysis** is a risk identification technique which is performed using the SWOT matrix.
- It is popularly used by PM. Often organizations implement SWOT analysis in their risk management strategies.
- **SWOT** stands for Strengths, Weaknesses, Opportunities, and Threats, and it aims to identify any opportunities for the project that may emerge from organizational qualities, and any threats emerging from organizations' shortcomings.
- The **SWOT framework** is used by organizations and teams for assessing the internal and external influences. These influences may have an impact on a project, product, or an institution in a positive or negative way.

7.5 CYBERSECURITY RISK IDENTIFICATION AND MANAGEMENT

- The analysis is useful in identifying internally-generated risks that arise from within the organization.
- **SWOT examination** is more about the association than the task. It contributes immensely in strategic decision making and is commonly used to manifest important project information to management.
- This technique has proven to encourage management for altering some environmental factors from the strengths and weaknesses sections that may have an impact on the project.

STRENGTH	WEAKNESS
OPPORTUNITY	THREAT

FIGURE 6.3 SWOT matrix.

7.5 CYBERSECURITY RISK IDENTIFICATION AND MANAGEMENT

- A **SWOT examination** can likewise be used for deciding the internal and external factors that may be beneficial or detrimental to a business venture.
- SWOT analysis for the team may be used to address the team's challenges for sustainment and growth. A SWOT analysis is usually performed with a team leader or an entire team.
- **During SWOT analysis**, it is important to capture all ideas so that everyone on the team must have a good understanding regarding the risks to the team.
- Once the analysis is performed, the team presents action plans for addressing the issues that were identified during the analysis. This can significantly improve the likelihood of success and sustainment for the team.

7.5 CYBERSECURITY RISK IDENTIFICATION AND MANAGEMENT

- The Strengths and Weakness analysis focuses on issues within the organization (internal), while Opportunities and Threats are usually focused on external factors.
- A SWOT analysis consists of items captured in a four-box layout.
- Strengths and Weaknesses are listed in the top 2 boxes, while opportunities and threats are listed in the bottom 2 boxes.

STRENGTH	WEAKNESS
OPPORTUNITY	THREAT

FIGURE 6.3 SWOT matrix.

Chapter

07

7.7 RISK ANALYSIS

- **Risk analysis** refers to the survey of the risks related to a specific occasion or activity.
- Risk analysis is important for ventures, innovation, technology, security issues, and any activity where risks need to be analyzed quantitatively and qualitatively.
- Risk analysis may be thought of as a component of risk management as risks are part of technology-driven projects and business endeavors. Therefore, it is imperative that risk analysis occurs on a recurring basis.
- There is a need to update risk analysis for accommodating new potential threats. Strategic risk analysis can adequately diminish harms and future risk probabilities.
- **Risks** can be associated with individuals who use computers incorrectly or inappropriately, as this may lead to security risks.
- There is risk associated with ventures that are not finished in a timely manner, since this leads to significant costs.

7.7 RISK ANALYSIS

- Risk analysis may be of two types to identify risk : **qualitative** and **quantitative**.
- **Quantitative risk analysis (QRA)** measures the expected risk likelihood to measure assessed money-related misfortunes from possible risks.
- **Qualitative risk analysis** does not utilize numbers however surveys threats and decides and sets up risk mitigation techniques and arrangements.
- **QRA** relies on pre-existing relevant and verifiable data. This data is used to produce a numerical worth which is then used to foresee the likelihood of a risk event outcome.
- **Qualitative risk analysis** relies on subjective assessment of risk occurrence likelihood (probability). This probability is measured against the potential severity of the risk outcomes (impact) to determine the overall severity of a risk.

7.7 RISK ANALYSIS

- Every organization requires a risk management strategy. This makes cyber risk assessment a crucial part of any company or organization.
- Every organization these days depends on innovation, technology, and information systems to lead business.
- **Cyber risk assessment** refers to performing an assessment of the cyber risks faced by companies or organizations.
- According to NIST, **Risk assessments** can identify, estimate, and prioritize risks for organizational operations. These operations may be missions, functions, image, and reputation.
- Cyber risk assessment may be used to assist decision-makers and to support proper risk responses.

7.8 RISK ASSESSMENT

- Since chiefs and executives cannot dive into security risks on an everyday basis, cyber risk evaluation may act as a kind of executive summary to enable those parties to make informed decisions about security.
- Some possible ways to do that is by identifying the significant threats to your organization:
 - Internal and external vulnerabilities
 - Impact if those vulnerabilities are exploited
 - Likelihood of exploitation.

7.8 RISK ASSESSMENT

- There are various **purposes behind performing a cyber risk assessment**, some of them are:
 - They can reduce long-term costs.
 - It gives a layout to future evaluations.
 - They provide an organization with greater self-awareness: knowing where your organization's weaknesses lie may provide a better idea of what areas the organization needs to grow and invest in.
 - It helps avoid breaches and other security incidents.
 - It can improve communication.
- Cyber risk assessment relies on input from many different departments and stakeholders. This may ensure organizational visibility and strengthen communication.

7.8 RISK ASSESSMENT

- Ideally, an association would have a workforce in-house that could deal with this sort of evaluation.
- Further, there must also be information that high-level executives understand and potentially proprietary organizational information that may be useful during the assessment.
- Cyber Risk assessment does not ignore organizational visibility.
- However, small or medium-sized businesses may need to outsource the assessment because they might not have the right people to do the job in-house. In that case, a third party might have to do it.
- Such services can be provided by companies as well as individual consultants.
- Over the last few years, many IT risk-assessment frameworks have been introduced with the objective of guiding security and risk executives.

7.5 CYBERSECURITY RISK IDENTIFICATION AND MANAGEMENT

OCTAVE

- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a risk assessment methodology that aims to recognize, oversee, and assess data security risks.

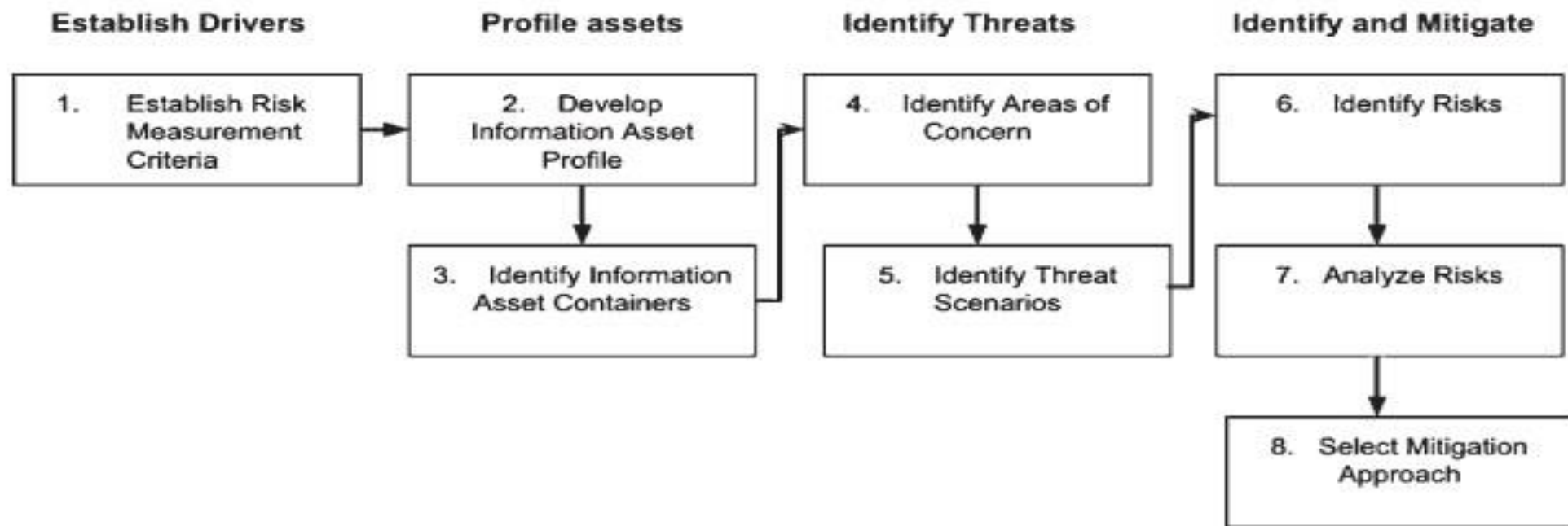


FIGURE 6.9 OCTAVE methodology and activity areas.

Chapter

07

7.10 RISK MANAGEMENT

- **Risk management** defined as the progressing procedure of distinguishing, evaluating, and reacting to risk.
- It must take an expansive perspective on risks over an association to inform resource allocation, better manage risks, and empower responsibility.
- Cybersecurity risk management is basically real-world risk management applied to the cyber world. It includes recognizing risks and vulnerabilities in an association and applying authoritative actions and comprehensive solutions to ensure that the association is satisfactorily secured.
- Risk management basically involves identifying potential risks. However, it also refers to assessing the impact of the risks, and planning how to respond if the risks become reality.
- Therefore, every organization or industry, despite its size, must develop a **cybersecurity risk management plan.**

Chapter

07

7.10 RISK MANAGEMENT

- However, it is also necessary to understand that not all risks, even if identified in advance, can be eliminated.
- It is possible to reduce the potential impact of risks.
- **Risk management** deals with four important **spheres**:
 1. **Accepting Risks:** Acknowledging that risks exist, but applying no safeguards
 2. **Transferring Risk:** Shifting responsibility for the risk to a third party
 3. **Avoiding Risks:** Eliminating the asset's exposure to risk or eliminating the asset
 4. **Mitigating Risk:** Modifying the asset's risk exposure and applying shields.

7.10 RISK MANAGEMENT

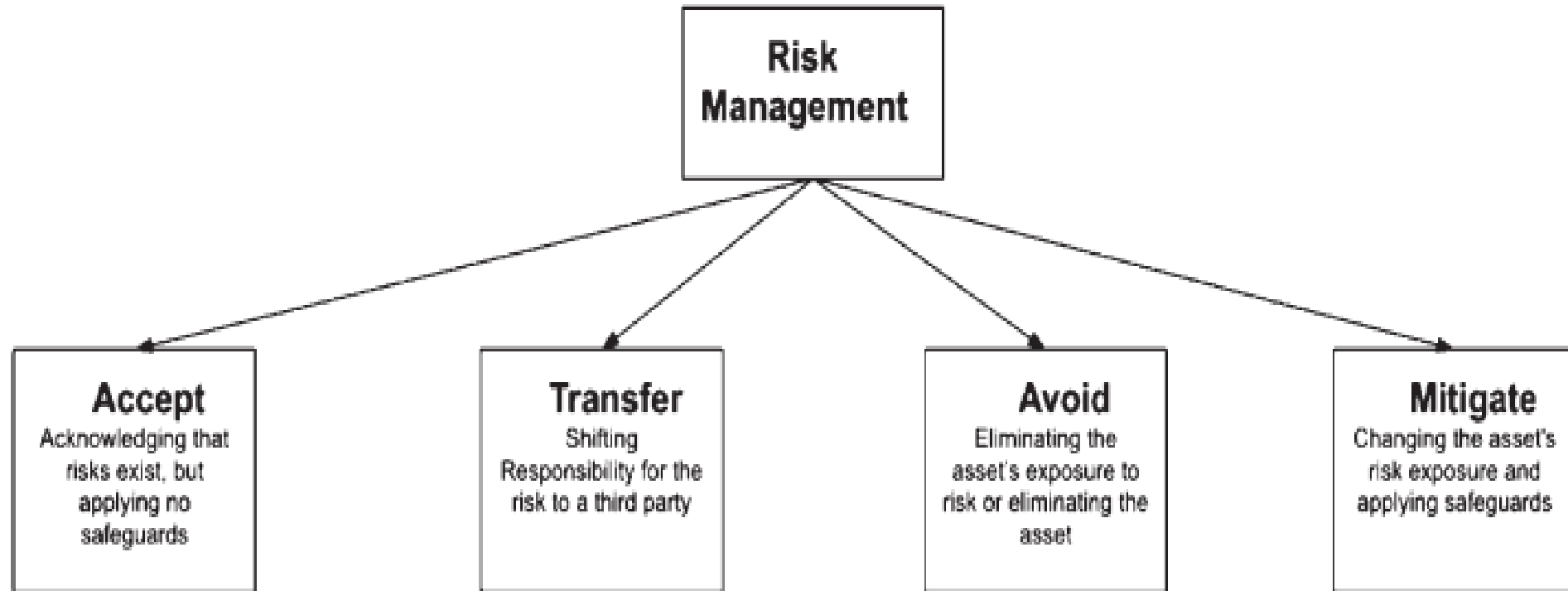


FIGURE 6.10 Risk management spheres.

7.10 RISK MANAGEMENT

- In order to plan risk management for an organization some points must be considered:

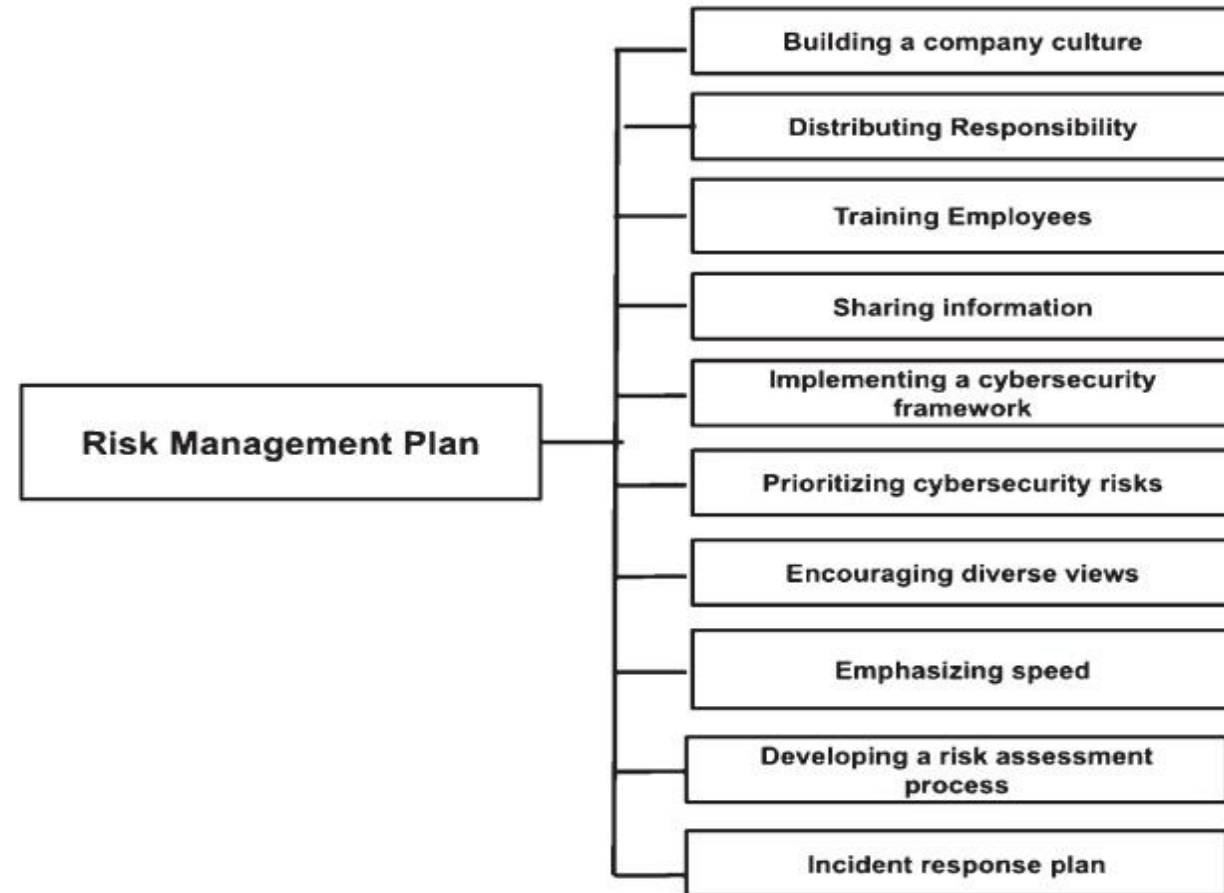


FIGURE 6.11 Risk management plan.

7.11 RISK MANAGEMENT FRAMEWORK (RMF)

- **Risk management framework (RMF)** is a structure that brings a risk based, full-lifecycle way to deal with the usage of cybersecurity.
- RMF takes into account the integration of cybersecurity in the systems design process. This results in a more reliable framework that can constantly work even with a proficient cyber adversary.
- PM must ensure that cybersecurity risks are managed consistently with framework execution prerequisites and are adequate to the service-assigned Authorizing Officials (AO).

7.11 RISK MANAGEMENT FRAMEWORK (RMF)

1. **Confidentiality:** The property that information is not unveiled to system entities (users, processes, devices) except if they have been approved to get to the data.
2. **Integrity:** The property whereby an entity has not been modified in an unauthorized manner.
3. **Availability:** The property of being accessible and usable upon demand by an authorized entity.

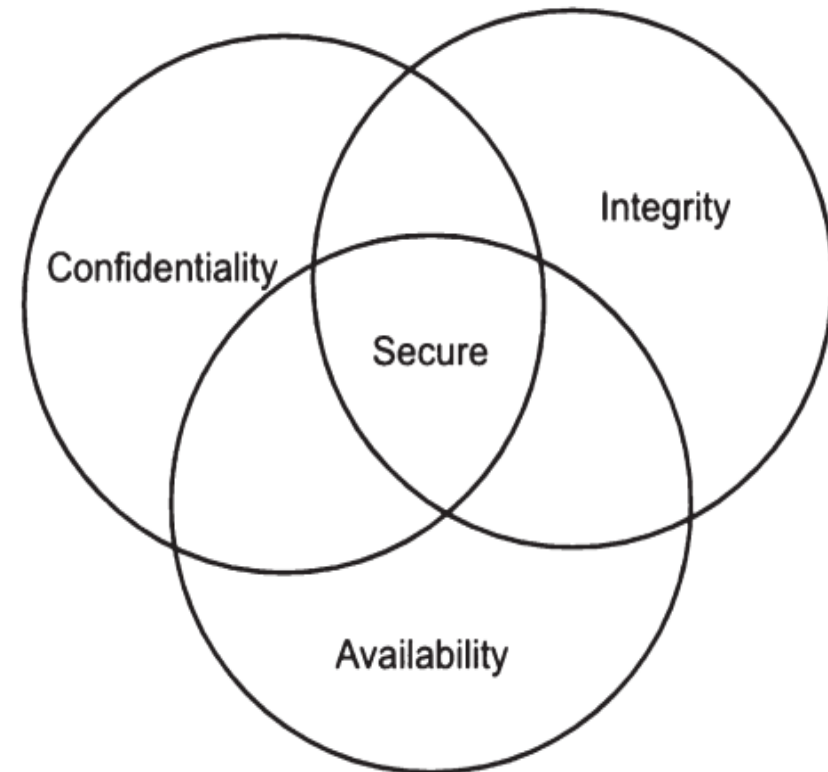


FIGURE 6.13 Cybersecurity requirements.

Chapter
07

7.11 RISK MANAGEMENT FRAMEWORK (RMF)

- 7.11.1 NIST RISK MANAGEMENT FRAMEWORK (RMF)

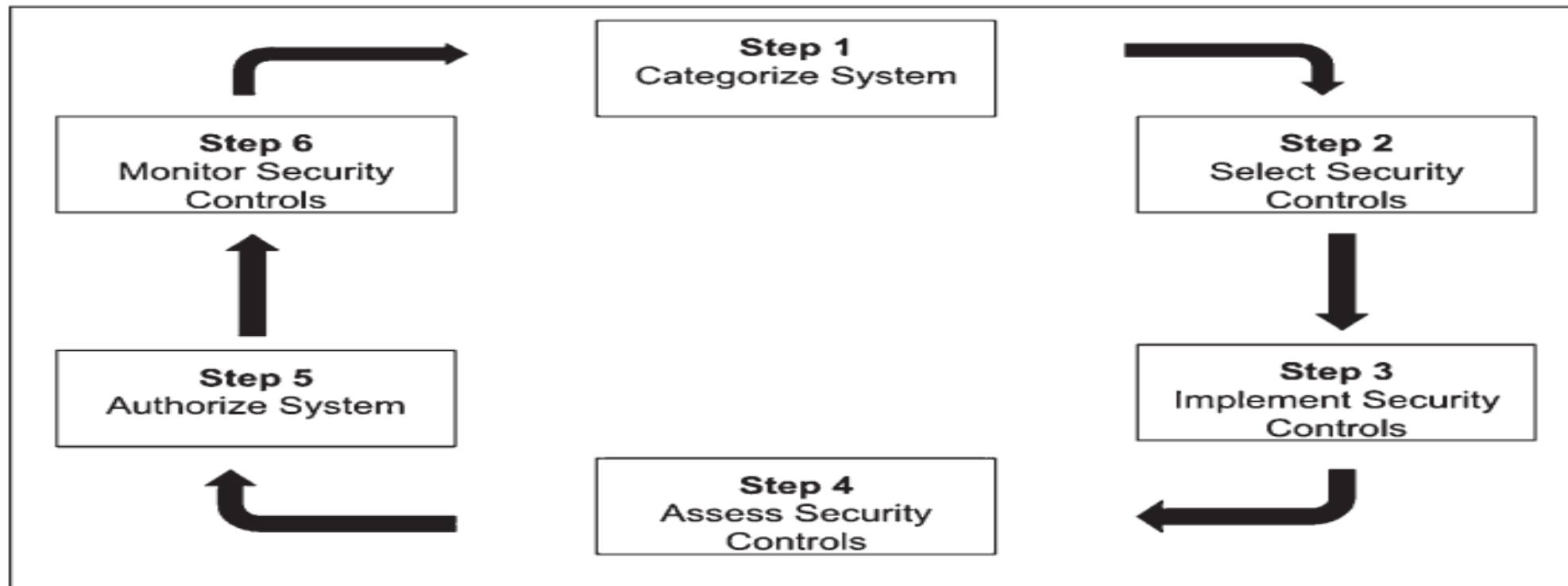


FIGURE 6.14 NIST risk management framework (RMF).

7.11 RISK MANAGEMENT FRAMEWORK (RMF)

- 7.11.2 ISO 31000 STANDARDS

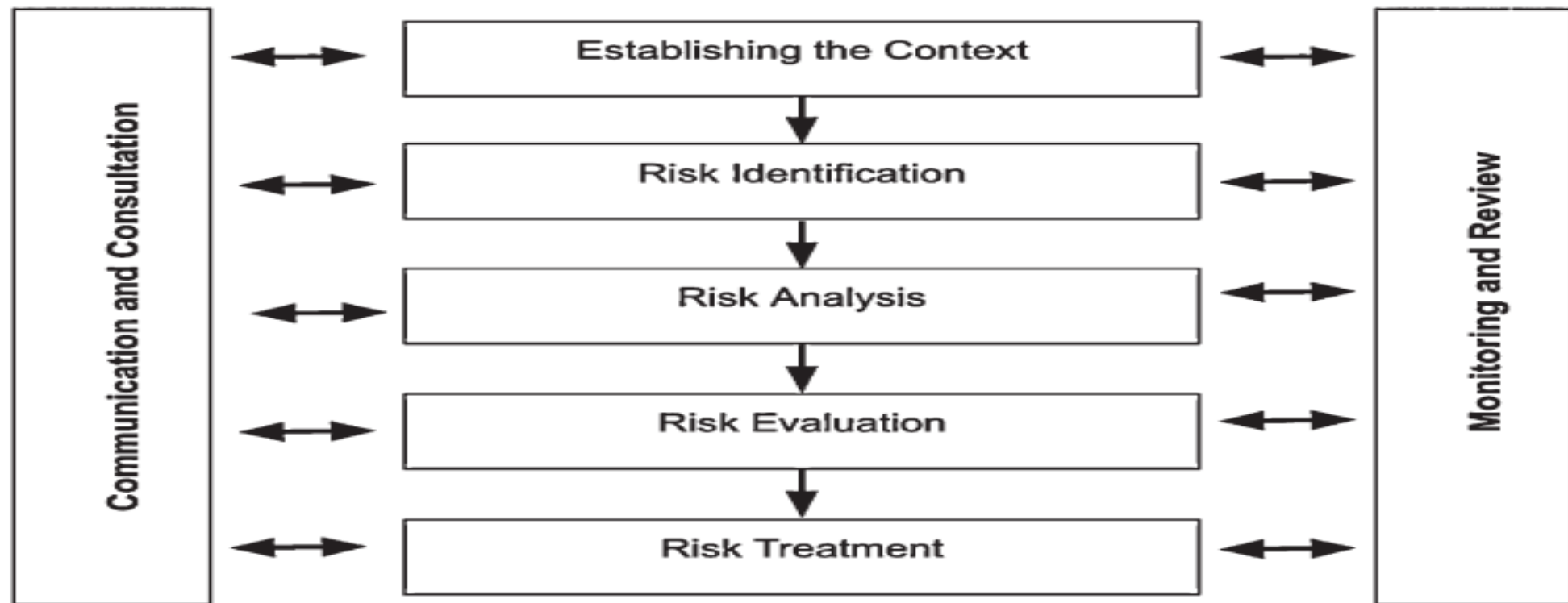


FIGURE 6.16 Risk management process for ISO 31000.

7.12 RISK REMEDIATION

- **7.12 RISK REMEDIATION**
- **Remediation** in cybersecurity refers to tending to a breach and restricting the extent of damage that breaches can possibly cause to your business.
- Threat remediation is popularly used for fighting cybersecurity compromises. The process of remediation involves the treatment of a security breach.
- Using remediation techniques, it is possible to dispense a malevolent assaults as malware, ransomware, phishing, and such.

7.12 RISK REMEDIATION

- **7.12 RISK REMEDIATION**

- If timely actions are not taken against breaches, they can grow massive such that it may be impossible to contain them. Thus the valuable data that belongs to a particular business can be compromised.
- Many remediation procedures these days act as elementary techniques to the gargantuan security incidents. For example, many remediation solutions trigger an automated kill process. While killing the problematic process may seem like the ultimate solution, it must be viewed as what sort of threat as well as breach is answerable for the problematic process.

7.12 RISK REMEDIATION

- **7.12 RISK REMEDIATION**

- Regardless of whether the dubious activity is killed, the attackers can remain in the system and network. In order to end the problem, the proposed remediation processes must **consider the detection of the cause**.
- Numerous remediation procedures cannot totally confirm if the threat is completely eradicated. Therefore, the remediation processes employed by the security teams must include gathering exact and sufficient data concerning the incident. Remediation is extremely essential for cyber-security.
- Most of the security compromises take more than a month to detect.

7.12 RISK REMEDIATION

- **7.12 RISK REMEDIATION**
- There are a few of the **operational difficulties** that associations face in building up and maintaining a reasonable cybersecurity risk remediation program.
- **These difficulties include:**
 - Characterizing risk baselines
 - Setting up a technique for risk prioritization
 - Optimizing risk remediation processes
 - Developing reliable and valuable metrics



Thank You