Risk Management

Introduction

You have just finished your work, prepared a hot cup of coffee, and decided to finish a new room on your favourite cyber security training platform. Now you want to enjoy your coffee while completing the room's tasks; however, you pause momentarily and think, "What if the coffee spills on your desk and gets on your keyboard?" You can consider one of the following:

- Enjoy your coffee before you finish a few more tasks. This way, you ensure that there is no way that coffee would get inside your keyboard.
- Drink your coffee while doing new tasks. No matter how small, there is a chance that your coffee mug might spill and your keyboard would need to be serviced (or replaced).
- You decide you cannot work without coffee, so you visit a nearby computer store and get yourself a keyboard protector or even a spill-resistant keyboard. This way, any coffee spill won't cause any damage.

Every activity entails some level of risk. In layperson's terms, the risk is the possibility that something unwanted or harmful might happen due to an action or event. This thought process does not require any formal study of risk management. However, all three routes explored above can be valid responses to risks. In this case, it is the risk of spilling liquid on your keyboard.

- If you decide not to bring coffee anywhere near your desk, that would be risk avoidance.
- Drinking coffee while working with full knowledge of the risk would fall under risk acceptance.
- Finally, upgrading your keyboard would be a risk reduction.

Responses to risk will be explored and discussed in detail in a later section; however, we hope that this example from everyday life intrigues you to learn more about risk management formally.

We will revisit this in more detail; however, risk management is a process of identifying, assessing, and responding to risks associated with a particular situation or activity. In Information Systems, risk management deals with threats to a computer system and its resources.

Room Prerequisites

This room has no strict prerequisites; however, studying it along with the Security Governance and Regulation and Threat Modelling rooms would be helpful.

Learning Objectives
By the end of this room, you will have learned about the following:

- Vulnerability, Threat, and Risk
- Information Systems Risk Management
- Risk Management Process: Frame, Assess, Respond, and Monitor
- Deciding how to respond to a risk

****

Answer the questions below:

You have registered to attend a local workshop about offensive cyber security tools. The workshop requires the attendees to bring their own laptops. This workshop is critical for you, and you want to get the most out of it. Your laptop is good and reliable; however, as with any electronic device, there is always a chance, no matter how minuscule, that something might go wrong and it would fail.

You decide to carry an extra laptop; if your main laptop fails, the second laptop will be ready. What would you call this response to risk?
Answer: Risk Reduction

You think your laptop has never failed before, and the chances of failing now are too slim. You decide not to take any extra actions. What do you call this response to risk?
Answer: Risk Acceptance

Basic Terminology

Before starting, it is essential to define the main terms to avoid ambiguity or confusion. To study risk management, we need to ensure a proper understanding of the following terms:

- Threat: an intentional or accidental event that can compromise the security of an information system. Examples include hacking, phishing attacks, human error, and natural disasters.
- Vulnerability: a software, hardware, or network weakness that cybercriminals can exploit to gain unauthorised access or compromise a system.

- Asset: a valuable resource or component (tangible or intangible) that an organization relies upon to achieve its objectives.
- Risk: the probability of a threat source exploiting an existing vulnerability and resulting in adverse business effects.
- Risk Management (RM): the process of identifying, assessing, and mitigating risk to maintain acceptable levels.

Threat

A threat is a potential harm or danger to an individual, organization, or system. Threats can be classified into three main categories: human-made, technical, or natural.

Human-made threats: These threats are caused by human activities or interventions. Examples include:

- Terrorism
- Wars and conflicts
- Riots and civil unrest
- Cyberattacks
- Industrial accidents
- Arson

As can be seen, human-made threats are not limited to cyberattacks; although they do not require technical expertise, arson is a grave threat. Realising any of these threats can have the power to disrupt the whole business; both a cyberattack and arson can prevent a company from functioning for a while.

Technical threats: These threats result from technological failures, malfunctions, or vulnerabilities. Examples include:

- Power outages
- Software and hardware failures
- Data breaches
- Network and system vulnerabilities
- Equipment malfunctions

A power outage can halt an entire company without a backup power source. A failed power supply means the whole server is down unless another backup power supply is on standby. Any of these technical threats can prevent business processes from moving forward; therefore, considering each of these threats is a must in any risk analysis.

Natural threats: These are threats caused by natural events or phenomena. Examples include:

- Earthquakes
- Floods

Natural threats depend on the location of the company or data centre. Studying the natural hazards to which a particular area is exposed is necessary to ensure proper risk analysis.

Vulnerability
A vulnerability is a weakness in the system or software that can be exploited by a threat to cause harm. To elaborate, it is a weakness that can be exploited by malicious individuals, groups, or external factors to gain unauthorized access, cause damage, or compromise the integrity, availability, or confidentiality of a system, data, or network. Vulnerabilities can arise from software bugs, misconfigurations, or outdated security.

Asset
An asset is an economic resource owned or controlled by an individual, company, or government. It typically has the potential to provide some future benefit. Assets include cash and cash equivalents, accounts receivable, investments, stock, equipment, real estate, and intellectual property.

In the context of information systems, an asset in information systems refers to any valuable resource or component (tangible or intangible) that an organization relies upon to achieve its objectives. These assets are critical for successfully operating and managing the organization's information processes.

Some examples of assets in an information system include:
- Hardware: Servers, workstations, routers, switches, firewalls, and other physical devices used to store, process, and transmit information.
- Software: Operating systems, applications, databases, and other programs that enable the organization to perform its functions efficiently and effectively.
- Data: Organizational data, which includes sensitive information such as customer records, financial data, intellectual property, and personal data of employees.
- Documentation: Manuals, policy documents.

Risk
Risk is the probability of a threat source exploiting an existing vulnerability (in an asset) and resulting in adverse business effects.

Risk is the potential of encountering unforeseen events or circumstances that may lead to a loss, damage, or negative outcome. It is the possibility of an undesirable

consequence from an uncertain situation, and it can be present in various aspects of life, such as finance, health, and personal relationships. In a business context, it is the probability of a threat source exploiting an existing vulnerability and resulting in adverse business effects. Since the existence of assets is taken for granted, some references omit assets from the visual representation.

In information systems, risk refers to the potential threats, vulnerabilities, and negative consequences arising from the interaction between IT infrastructure, software applications, data, and users. It deals with the uncertainties organizations face in ensuring their digital assets' confidentiality, integrity, and availability.

Risk Management

As mentioned earlier, risk management is a process of identifying, assessing, and responding to risks associated with a particular situation or activity. It involves identifying potential risks, assessing their likelihood and impact, evaluating possible solutions, and implementing the chosen solutions to limit or mitigate risk. It also involves monitoring and assessing the effectiveness of the solutions put in place.

A Risk Management Policy is a set of procedures and processes designed to minimise the chances of an adverse event or outcome for an organization. It helps organizations identify, assess, and manage potential and actual risks related to their operations, financial activities, and compliance with applicable laws and regulations. The policy provides guidance on identifying and assessing risks, as well as assigning tasks and responsibilities to those involved in managing them.

Information Systems Risk Management is a system of policies, procedures, and practices that seek to protect a company's computer system from various internal and external threats. It includes identifying threats, assessing the probability of their occurrence, and evaluating the effectiveness of various measures that can be taken to limit the damage they could cause. The process also involves determining the resources that should be allocated to respond to potential threats, as well as monitoring and maintaining the integrity of the system.

****

Answer the questions below:

What do you call the potential for a loss or an incident that may harm the confidentiality, integrity or availability of an organization's information assets?

Answer: Risk

What do you call a weakness an attacker could exploit to gain unauthorised access to a system or data?
Answer: Vulnerability

What do you consider a business laptop?
Answer: Asset

Ransomware has become a lucrative business. From the perspective of legal business, how do you classify ransomware groups?
Answer: Threat

Risk Assessment Methodologies

There are several frameworks for risk assessment. Example methodologies are:

- NIST SP 800-30: A risk assessment methodology developed by the National Institute of Standards and Technology (NIST). It involves identifying and evaluating risks, determining the likelihood and impact of each risk, and developing a risk response plan.
- Facilitated Risk Analysis Process (FRAP): A risk assessment methodology that involves a group of stakeholders working together to identify and evaluate risks. It is designed to be a more collaborative and inclusive approach to risk analysis.
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE): A risk assessment methodology that focuses on identifying and prioritising assets based on their criticality to the organization's mission and assessing the threats and vulnerabilities that could impact those assets.
- Failure Modes and Effect Analysis (FMEA): A risk assessment methodology commonly used in engineering and manufacturing. It involves identifying potential failure modes for a system or process and then analyzing the possible effects of those failures and the likelihood of their occurrence.

Based on NIST SP 800-30, the risk management process entails four steps:

1. Frame risk: First, we must establish the context within which all risk activities occur.
2. Assess risk: We must identify, analyze, and evaluate potential risks and their likelihood and impact. This step is crucial to help decide on a proper response later.

3. Respond to risk: We need to take the steps necessary to mitigate the likelihood or impact of the risk. The response depends on many factors, and we will cover them separately.
4. Monitor risk: Finally, we continue tracking and evaluating the effectiveness of risk responses, identifying new risks, and ensuring that our risk management activities are effective. Monitoring is an ongoing process, as many criteria might change over time.

We will discuss each in its own task.
****

Answer the questions below:

What is the name of the risk assessment methodology developed by NIST?
Answer: NIST SP 800-30

Frame Risk

Risk management begins with establishing a risk context, i.e., framing risk. The purpose of risk framing is to develop a risk management strategy.

Organizations must define a risk frame to set the groundwork for managing risk and provide limits to risk-based decisions. To create a reasonable risk frame, organizations must identify the following:

- Risk Assumptions: What are the assumptions about threats and vulnerabilities? What is the likelihood of occurrence? What would be the impact and consequences?
- Risk Constraints: What are the constraints on assessing, responding, and monitoring risks?
- Risk Tolerance: What are the acceptable levels of risk? What is the acceptable degree of risk uncertainty?
- Priorities and Trade-offs: What are the high-priority business functions? What are the trade-offs among the different types of faced risks?

Example Scenario

Consider the case where you are part of the risk management team for an accounting company, and let's revisit the above questions. We will avoid discussing risks and threats common to every company using information systems. In this example, we will only focus on one risk: data theft.

- Risk Assumptions: The fact that this company handles the accounting data of its clients increases the risk of being targeted by adversaries that would try to profit

from stealing such data. Unless proper measures are taken, the likelihood of success is relatively high, and the impact would be disastrous for the company's image.

- Risk Constraints: The primary constraints are expected to be budget-related. Safeguarding the data requires improving physical and cyber security; it entails conducting cyber security training and hiring new personnel.
- Risk Tolerance: Considering the type of business, the risk of data theft cannot be tolerated. Tolerating data theft would lead to the whole company going out of business.
- Priorities and Trade-offs: The priority is to maintain a trustworthy image of a company that can conduct its business with confidentiality and integrity.

****

Answer the questions below:

Make sure you have read the above.
No Answer Needed

Assess Risk

Risk assessment is the second part of risk management, which involves examining risks within the organization's risk framework.

The goal of the risk assessment is to determine the following:

- Threats: What are the threats that you need to consider?
- Vulnerabilities: What are the vulnerabilities that you have to deal with?
- Impact: What would be the impact if a threat exploited a vulnerability?
- Likelihood: What is the likelihood of this vulnerability being exploited?

Threats

Various risk types exist because threats range from human beings to natural causes. We have already listed the types of threats in Task 2. In the following two examples, we will consider the following two threats:

- Physical damage: From natural causes to human-made, accidents happen. Examples include water leakage, fire, and power loss.
- Outsider threat: There are always adversaries interested in your systems; even if your data is only valuable to you, they can still try to infect your system with ransomware.

Example 1

Let's consider the following example for assessing one natural threat, a tsunami. The company's main office is at ground level and overlooks the beach. That would make it vulnerable to tsunamis that can literally wash every single piece of equipment and paper inside the office. However, the country has never experienced tsunamis in its entire written history, and geologists state that the probability of a tsunami happening is negligible. In this scenario, we have:

- Threat: Tsunami
- Vulnerability: The office is near the seashore
- Impact: Destruction of office equipment
- Likelihood: Negligible

Example 2

One academic institution offers quality education for its students via its undergraduate and graduate programs. Although the faculty and their students conduct research, they are of purely academic worth and cannot be monetised. In other words, no entity would be interested in stealing their research. Does this make them safe? Not really. With the spread of ransomware groups, a threat actor would encrypt their data servers and try to blackmail them into paying. The impact of such an attack would force the university to close for a few hours or days till all data is recovered from the backup, assuming it exists. The likelihood of being targeted is high, especially since this university is prestigious and well-known.

- Threat: Ransomware Groups
- Vulnerability: Data is stored on computer systems
- Impact: Disrupting the work of faculty and staff (till the data is recovered from backup)
- Likelihood: High

****

Answer the questions below:

Make sure you have read the above.

No Answer Needed

Risk Analysis

We have two approaches when it comes to risk analysis:

- Qualitative Risk Analysis, where we assign ratings to risks. The ratings can be a qualitative adjective, such as high, medium, and low. Alternatively, it can be something symbolic, such as red, yellow, and green.
- Quantitative Risk Analysis, where we assign monetary values and use that as a basis for decision-making.

Qualitative Risk Analysis

As the name suggests, qualitative risk analysis uses qualitative adjectives to describe:

- Probability of a risk-taking place, i.e., probability of a threat exploiting a vulnerability
- Impact of the risk, if realised, which can range between trivial to extreme

The figure below shows a table matching impact with probability. We would allocate fewer resources to respond to a risk that is unlikely to occur and has a trivial effect; however, it is the opposite case if the risk is likely to occur and has a significant impact. The former case is a low risk, while the latter is a high risk. Consequently, the response is decided accordingly.

		Impact				
		Trivial	Minor	Moderate	Major	Extreme
Probability	Rare	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very Likely	Medium	Medium	High	High	High

Quantitative Risk Analysis

Single Loss Expectancy

Using quantitative analysis, we need to assign monetary values and numeric percentages. Let's start with the following equation:

- $SLE = AssetValue \times EF$

Where:

- Single Loss Expectancy (SLE) is the loss incurred due to the realization of a threat represented as a monetary value.
- Asset Value is the monetary valuation of an asset

- Exposure Factor (EF) is the percentage of loss a realised threat can cause to an asset.

SLE Numeric Example

Consider the following numeric example for a work laptop considering the threat of a ransomware virus.

- Asset Value = $10,000; the laptop is worth $1000, and the data are worth $9000.
- EF = 90%; a ransomware infection would cause all the data to be unusable.

Consequently,

- $SLE = AssetValue \times EF = \$10,000 \times 90\% = \$9,000$.

In other words, a ransomware infection for such a work laptop would cause the company to lose $9000, assuming there is no backup copy.

Annualized Loss Expectancy

However, this information is insufficient for us to decide on countermeasures. We need to find the expected loss per year.

- $ALE = SLE \times ARO$

Where:

- Annualized Loss Expectancy (ALE) is the loss the company expects to lose per year due to the threat.
- Annualized Rate of Occurrence (ARO) is the expected number of times this threat is realised yearly, i.e., frequency per year.

Why do we need to calculate ALE? ALE helps us decide whether paying for a particular control or safeguard is justified, as we will see in Task 7.

ALE Numeric Example

Let's revisit our example and calculate the ALE.

- We have already calculated the SLE as $9000; we need to figure out how often we expect this incident to happen yearly.
- Based on experience, a work computer is infected with ransomware once every two years. Hence, the annualized rate of occurrence is 0.5.

Consequently,

- $ALE = SLE \times ARO = \$9000 \times 0.5 = \$4,500.$

In simple terms, we expect the ransomware threat to cost us $4500 per laptop per year unless we take proper measures.

****

Answer the questions below:

Ensure you have noted the mathematical formulas and the acronyms presented here, as they will be necessary to conduct quantitative risk analysis in later tasks.
No Answer Needed

Respond to Risk

Risk management's third component focuses on how organizations respond to the risks identified through risk assessment. What are the possible responses to risks?

- Avoid Risk
- Transfer Risk (or Share Risk)
- Mitigate Risk (or Reduce Risk)
- Accept Risk

The response you choose against the risk takes into account the severity of the threat, the probability of occurrence, and the costs of the possible countermeasures. Let's cover each in more detail.

- Avoid Risk: If a company decides to eliminate the activity that leads to the risk, that would be risk avoidance. A bank might decide that all employees' computers cannot access the Internet to protect its systems against all online threats. An organization might instruct its employees to work exclusively using the workstations on its premises to prevent data from being stolen.
- Transfer Risk: A company might consider the risk too high to handle, so it decides to purchase insurance. That would be risk transference or risk sharing. A publishing house might buy insurance against fire, for instance.
- Mitigate Risk: A company might invest in countermeasures to reduce risk to an acceptable level; this would be risk mitigation. To protect against computer viruses, a company might install antivirus on all its computers instead of blocking access to the Internet and gluing the USB ports.
- Accept Risk: Sometimes, the countermeasure cost exceeds the loss incurred if the risk is realised.

It is important to stress that "Ignore Risk" is not a valid choice. Accepting a risk does not mean the risk is ignored. It means the risk is analysed along with its impact and countermeasures; however, some reasons justify keeping things unchanged. One reason might be that the countermeasure is too expensive compared to the potential loss. Another reason might be that implementing a countermeasure would significantly alter the business process.

Quantitative Analysis

Quantitative risk analysis would help us decide whether a specific control is justified from the business perspective. Implementing a safeguard won't make sense unless its benefit outweighs its cost.

Consider again our example of the risk of a laptop getting infected by ransomware. Can we mitigate this risk? We are considering setting up antivirus software on all laptops. The cost is $120 per laptop annually, including the licensing and extra staff hours.

We need to decide whether this countermeasure is justified from the business perspective. To do that, we need to calculate the value of the safeguard. It would be justified from the business perspective only if the value of the safeguard is positive. The value of the safeguard to the organization is calculated as follows:

- $ValueofSafeguard = ALEbeforeSafeguard - ALEafterSafeguard - AnnualCostSafeguard$

We have already calculated ALE before the safeguard is implemented.

- $ALEbeforeSafeguard = SLEbeforeSafeguard \times ARObeforeSafeguard = \$9000 \times 0.5 = \$4,500.$

Let's calculate ALE after the safeguard is added:

- $ALEafterSafeguard = SLEafterSafeguard \times AROafterSafeguard$

We might need to recalculate SLE in case the implemented safeguard affected the exposure factor (EF):

- $SLEafterSafeguard = AssetValue \times EFafterSafeguard$

In this case, the exposure factor (EF) is not expected to change. In other words, installing an antivirus won't change the damage that a ransomware infection would cause. Consequently, SLE remains the same after the safeguard is implemented:

- $SLEafterSafeguard = AssetValue \times EFafterSafeguard = \$10,000 \times 90\% = \$9,000.$

However, an antivirus would significantly decrease the annualized rate of occurrence (ARO). Let's say that this antivirus is so efficient that we expect that ARO to become 0.02.

Now we can calculate ALE after the safeguard is added.

- *ALEafterSafeguard = SLEafterSafeguard × ARObafterSafeguard = $9, 000 × 0.02 = $180.*

We already estimated the safeguard cost to be $120 per year. Therefore,

- *ValueofSafeguard = $4, 500 − $180 − $120 = $4, 200.*

Because the value of the selected safeguard is positive, we conclude that it is justified from the business perspective. In other words, from the risk analysis perspective, installing an antivirus has a value (benefit) of $4,200 to the organization.

If the value of the safeguard turns out to be negative, it means that the cost of the safeguard outweighs its benefits. Consequently, it won't be justified from a business perspective.

****

Answer the questions below:

Click on View Site. Decide whether each of the suggested safeguards (controls) is justified. Follow the instructions to retrieve the flag.

Answer: THM{Excellent_Risk_Management}

Monitor Risk

We have assessed the risk and responded with a proper measure; what's next? We need to keep monitoring risks. Many reasons dictate that we continue to monitor risk, even after an appropriate response has been implemented. The reasons include the following:

- Finding and adding new risks
- Eliminating risks that are no longer relevant
- Assessing our responses to existing risks

For the latter, monitoring risks activities requires a focus on the following areas:

- Effectiveness
- Change
- Compliance

Effectiveness Monitoring

Responding to an assessed risk does not mark the end of the story. A solution might be effective now but might become ineffective in the future.

Consider the following example: there is always a risk that employees might use weak passwords, which would threaten the whole network. Specific password complexity requirements are enforced to mitigate this risk. This solution should work excellently, shouldn't it? However, while monitoring the effectiveness of this measure, you might discover that many employees are resorting to writing their complex passwords on sticky notes. Such discovery shows that the implemented control, i.e., password complexity, has become ineffective.

Without effectiveness monitoring, there is no way to discover whether a control is still effective and whether a risk is still mitigated correctly.

Monitoring Change

"Change is the only constant in life." as Heraclitus, a Greek philosopher, is quoted as saying. When it comes to risk monitoring, changes might be due to one of the following:

- Change in business
- Change in information systems

Business change might include opening new branches, creating new positions, and acquiring other companies. Any business change might introduce new risks and render existing controls invalid.

The more noticeable change is the change in information systems. Adding new equipment or migrating to new systems would introduce new risks. Consequently, monitoring such changes is necessary to assess unknown risks that have arisen.

Compliance Monitoring

New laws might see light, new regulatory requirements might come into effect, and new policies might be enforced. Although the pace of change is not as fast as in other areas, these are still areas that the risk management team need to keep an eye on and monitor.

Another aspect that needs to be monitored is the audit findings. Failing to address audit findings can result in fines or stir legal action.

****

Answer the questions below:

You want to confirm whether the new policy enforcing laptop disk encryption is helping mitigate data breach risk. What is it that you are monitoring in this case?

Answer: Effectiveness

You are keeping an eye on new regulations and laws. What is it that you are monitoring?
Answer: Compliance

Supply Chain Risk Management

A supply chain is a sequence of suppliers that lead to the delivery of a product. In information systems, the product can be hardware, software, or service. Consequently, the risk is as follows:

- Risk associated with hardware: Depending on the importance of the target, a threat actor can add a hardware Trojan to an electronic device. As with software Trojans, the purpose is to provide unauthorised functionality.
- Risk associated with software: Software Trojans require access to the software to plant it. In the worst-case scenario, the attacker would succeed in adding the Trojan directly to the source code.
- Risk associated with services: The risk can range from downtime to data breaches. A company must ensure that the service provider has a good security program before using its service.

Example Scenario

Consider the case of an accounting firm. They offer many services, such as reviewing and analyzing financial statements, performing audits, and filing tax returns. To be able to carry out these services, example supplies they need include:

- Computers
- Accounting software
- Printers

They would also need some way to communicate with their clients, such as email. This firm bought its computers from a local shop that also offers maintenance. They got the accounting software from a company specialising in developing and customising accounting software. Finally, they got email service from one of the leading Internet providers. If we take a closer look at these three suppliers, we notice that they include the following:

- Hardware suppliers, such as computers
- Software suppliers, such as accounting software
- Service providers, such as email

Although this accounting firm might follow perfect measures to protect its assets, the risk might creep in from one of the suppliers. Consider the case where a threat actor

succeeds at installing a malicious piece of code within the accounting software. Or consider the case where the email provider gets its servers breached and all confidential communications exposed.

****

Answer the questions below:

Make sure that you have read the above.

No Answer Needed

Putting It All Together

****

Answer the questions below:

Click on View Site and follow the instructions to retrieve the flag. Remember that your decision should be based on the value of the safeguard to the organization, which is calculated as follows:

ValueofSafeguard = ALEbeforeSafeguard − ALEafterSafeguard − AnnualCostSafeguard

Answer: THM{OFFICE_RISK_MANAGED}