Unit 1: An Introduction to Security and Risk Management

1. Discuss the various definitions of risk.

Stoneburner et al. (2002) define risk as the possible harm from exploiting a vulnerability. ISO/IEC 31000 describes risk as the impact of uncertainty on objectives and can have positive and negative consequences on business objectives. Regarding information security, risks are the consequences a business faces when a threat exploits a vulnerability. Such risks may include loss of intellectual property, damage to brand reputation, loss of revenue, costs for remediation, injury to staff, and loss of faith from investors (Campbell, 2016).

Blakley et al. (N.D.) define risk as the possibility of an event that reduces a business's value. Every risk has a quantifiable cost, multiplied by the probability of an adverse event by the downside consequence. Kovaitė & Stankevičienė (2019) define risk as an event's potential to deviate from what was expected, which might have adverse effects like injury or loss. Steps can be taken to prevent these risks. Risk and uncertainty are often linked because uncertainty is necessary for development and change.

Moreover, risk is a state of uncertainty in which some potential outcomes could lead to negative consequences, such as loss, injury, or catastrophe. In other words, there is a chance that something terrible will happen. Each potential outcome is linked to quantified probabilities and losses to measure risk (Hubbard, 2020).

Because various scientific domains have distinct views and settings, there is no consensus on defining and understanding risk. Risk may be defined in several ways, including expected values and uncertainty, occurrences and consequences and uncertainty, or goals connected to the risk. Because of the constraints of standardisation organisations, scientific discourse, and current research, attempts to

develop a unified perspective on risk have not been broadly accepted (Šotić and Rajić, 2015.).

2. Explain how to assess, qualify and mitigate risks.

2.1. Risk assessment

A risk assessment is a decision-making tool performed by a competent person to identify, analyse, and control hazards and risks present in a situation. It aims to prioritise measures to eliminate or control risks based on their level of likeliness and impact. Risk assessment is a significant component of risk analysis, an ongoing process that identifies and analyses potential risks and issues detrimental to a business. Identifying hazards through risk assessment helps ensure the safety of employees and customers (Andales, 2023).

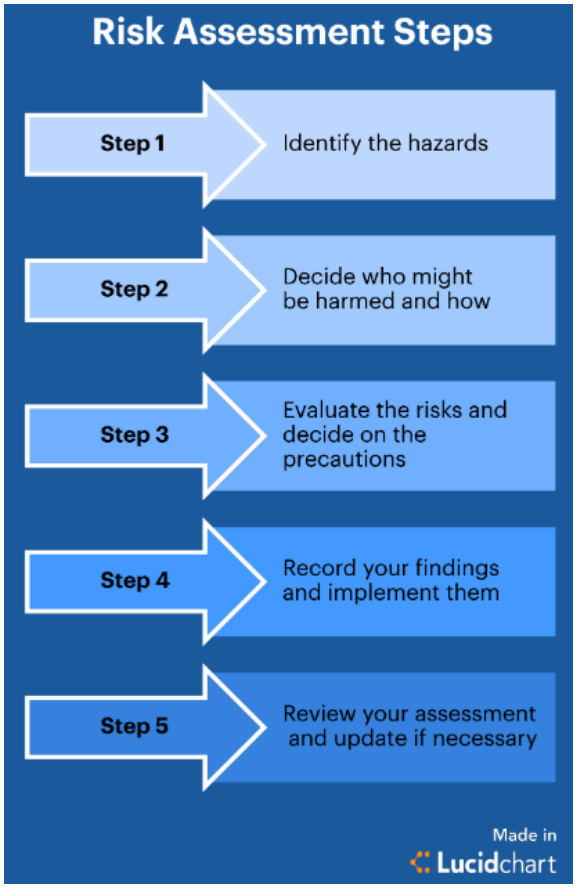
According to the Lucidchart Content Team (2018), a risk assessment is essential for organisations to prepare for and mitigate risks. It involves analysing potential threats, preventing injuries or illnesses, meeting legal requirements, and raising awareness about hazards and risks. Furthermore, it helps determine budgets, justify costs, and understand the ROI. Therefore, businesses must perform a risk assessment before introducing new processes or activities, changing existing ones, or identifying new hazards. The steps involved in risk assessment are critical components of any organisation's health and safety management plan.

British Safety Council (2023) note that to complete a thorough risk assessment, it is crucial to follow the HSE's recommended five-step process without exception. The steps are as follows:

- Identify potential hazards
- Determine who may be harmed by those hazards
- Evaluate the severity of the risk and establish appropriate precautions
- Implement changes and document your findings

- Review your assessment regularly and make revisions as necessary.

It can use observation, review records, consult manufacturer data sheets, or solicit employee input to identify potential hazards. Once hazards and potential harm have been identified, it must assess the severity of the risk and establish controls to mitigate it. It is essential to keep a record of the findings using a risk assessment form and to review the assessment periodically or following any significant event or near-miss.



Lucidchart (2018)

2.2. Risk Qualification

Choosing the proper risk assessment method can be challenging. Consider an organisation's expertise, technological infrastructure, tools, and data quality to ensure the most effective approach. Quantitative analysis is objective but requires more time and data, while qualitative analysis is quick but can be biased. Combining both strategies can improve the effectiveness and efficiency of the risk assessment process (Evrin, 2021).

Risk qualification is an essential aspect of risk management that involves estimating the likelihood of a risk occurring and assessing the severity of its potential impact. Qualitative terms such as "high," "medium," or "low", or quantitative scales like percentages may be used to determine the probability of a risk. On the other hand, the risk's impact is assessed by considering various factors such as financial losses, reputational damage, operational disruptions, and other consequences that may arise if the risk materialises (Graves, 2000).

According to Safran (2022), qualitative risk analysis enhances comprehension of project risks, helps to identify areas of exposure, and helps prioritise risks. Project managers may concentrate on developing solutions for the most critical risks and create a more comprehensive picture for the following projects by classifying risks according to their source and effect.

Gonzalez (2023) states that qualitative risk analysis involves several steps. The first step is identifying risks by noting them and asking team members for input. This can be done by holding brainstorming sessions or using a risk matrix to combine the consequences and likelihood of a risk occurring. Other techniques include assessing the causes and effects of each risk and preparing for different scenarios.

The second step is to control risks by focusing on the root causes of risks, such as hazards or inefficient management processes. This can be done through corrective actions like providing workers with PPE.

The final step is to monitor business risks by keeping notes on risks, risk ratings, and control measures. This helps in completing the last step of risk monitoring, which involves observing risks and asking questions about the effectiveness of risk control, correctly classifying risks, and identifying all risks.

Quantitative risk analysis is crucial for project managers to identify potential risks and their consequences. It involves specifying the analysis's purpose, scope, and method, which can be achieved through Failure Mode and Effects Analysis (FMEA), Business Impact Analysis (BIA), or Expected Monetary Value (EMV) methods. Project managers must ensure that the data, tools, and personnel are organised and compatible with the chosen method to prepare for the analysis. After applying the technique, recording and storing all results securely is crucial. This analysis can also benefit industry-specific functions like restaurant inspections, pharmaceutical audits, and food safety inspections (Gonzalez, 2023).

2.3. Risk Mitigation

Risk mitigation is identifying and reducing potential threats to a business or project. It involves developing a plan to manage or eliminate risks, minimise risk likelihood and implement strategies to respond to threats. It's essential to any business strategy, especially when facing outside risks beyond your control (Vige, 2022).

Wojno (2023) highlights that businesses face different types of risks: compliance, legal, strategic, reputational, and operational. Compliance and legal risks involve violating external or internal rules and regulations, which can lead to a loss of reputation or finances. Strategic risk is associated with a faulty business strategy, while reputational risk can damage a company's standing and lead to financial losses. Operational risk can occur from internal and external factors affecting a company's day-to-day activities and profits.

To successfully mitigate risks, one must take practical and assertive steps in the risk mitigation process, as emphasised by Wojno (2023):

1. Identify all potential risks impacting your project or business operations. Collaborate with stakeholders to ensure a comprehensive risk assessment.

2. Assess the likelihood and degree of negative impact each risk poses to your business. Categorise and prioritise risks based on their level of severity.

3. Treat the risks by implementing your chosen mitigation strategies and recording them in a risk register. Ensure that all stakeholders are aware of the plan and their roles in executing it.

4. Monitor the risks regularly to check their category and mitigation strategy. Use statistical tools to track project progress and identify changes in the risk profile.

5. Report on risks, best practices, and mitigation approaches to keep stakeholders informed. Communicate regularly to surface new risks and ensure that all decisions are made with a complete understanding of the risks involved.

3. Describe various approaches to quantify and qualify risks.

Simmons et al. (N.D.) state that risk analysis is a complex field that involves specialist knowledge and expertise. It is essential to have a comprehensive, transparent and accessible process. Various users, such as industrial and transport companies, regulators, and insurers, determine the methods used to analyse risks. There are two types of risk analysis methods: deterministic and stochastic. Deterministic methods consider the consequences of defined events, while stochastic methods attempt to capture all possible outcomes with their probabilities.

There are two main approaches to risk analysis: qualitative and quantitative. Qualitative risk analysis relies on expert judgment to evaluate risks based on their severity, likelihood, and urgency. Quantitative risk analysis involves numerical analysis and modelling to assess risks comprehensively (SOG, 2023).

SOG (2023) explains that quantitative approaches involve using numerical data and statistical analysis to assess risks. One such approach is the Failure Modes and Effects Analysis (FMEA), which consists of analysing a system's potential failure modes and their impact. Another quantitative approach is the Monte Carlo Simulation, which uses

statistical modelling to simulate various scenarios and assess the probability of different outcomes.

On the other hand, Manpreet (2023) explains that qualitative approaches do not rely on numerical data but instead focus on identifying and categorising risks based on their characteristics. A popular approach to qualitative risk assessment is the Risk Matrix, which plots likelihood and impact on a grid to prioritise risks visually. The SWOT Analysis is another qualitative approach that identifies strengths, weaknesses, opportunities, and threats, thus helping assess the overall risk profile. Finally, the Expert Judgment approach leverages the knowledge and experience of subject matter experts to evaluate risks based on their professional expertise and judgment.

4. **List common security and risk standards and select the appropriate one(s) for a given situation.**

Organisations rely on security frameworks to establish policies and procedures that safeguard against cybersecurity risks. These frameworks enable IT security professionals to maintain compliance and defend against cyber threats. Compliance must be regularly reviewed and updated to ensure continued security (Bonnie & Leach, 2024).

According to Bonnie & Leach (2024), there are various well-known security frameworks to select from. The common standards for managing security and risks in a particular situation include:

- **SOC 2**: This standard helps manage customer data.
- **ISO 27001** involves building and maintaining an Information Security Management System (ISMS).
- **NIST Cybersecurity Framework**: This standard identifies comprehensive and personalised security weaknesses.
- **PCI DSS**: This standard ensures the safety of card owner information.
- **HIPAA**: This standard protects patients' health information.

- **GDPR**: This standard ensures data protection for European Union residents.
- **HITRUST CSF**: This standard enhances security for healthcare organisations and technology vendors.
- **COBIT**: This standard aligns IT with business goals, security, risk management, and information governance.
- **CIS Controls:** This standard offers general protection against cyber threats.

References:

- Gary Stoneburner, Alice Y. Goguen, & Alexis Feringa (2002). Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology. [online] Available at: https://dl.acm.org/doi/book/10.5555/2206240 [Accessed 2 Feb. 2024].
- Campbell, T. (2016). *Practical Information Security Management*. 1st ed. John Wiley & Sons, Incorporated.
- Blakley, B., Mcdermott, E., Morganchase, J. & Geer, D. (N.D.). *Information Security is Information Risk Management*. [online] Available at: https://www.nspw.org/papers/2001/nspw2001-blakley.pdf.
- Kovaitė, K. & Stankevičienė, J. (2019). Risks of digitalisation of business models. *Proceedings of 6th International Scientific Conference Contemporary Issues in Business, Management and Economics Engineering '2019*. doi:https://doi.org/10.3846/cibmee.2019.039.
- Douglas W. Hubbard (2020). *The Failure of Risk Management: Why It's Broken and How to Fix It*. [online] Available at: https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2381255&site=ehost-live [Accessed 2 Feb. 2024].
- Šotić, A. and Rajić, R. (2015). *Online Journal of Applied Knowledge Management The Review of the Definition of Risk*. [online] Available at: https://www.iiakm.org/ojakm/articles/2015/volume3_3/OJAKM_Volume3_3pp17-26.pdf.
- Andales, J. (2023). *Risk Assessment Guide & Template Collection*. [online] SafetyCulture. Available at: https://safetyculture.com/topics/risk-assessment/.
- Lucidchart Content Team (2018). *A Complete Guide to the Risk Assessment Process | Lucidchart Blog*. [online] Lucidchart.com. Available at: https://www.lucidchart.com/blog/risk-assessment-process.
- British Safety Council (2023). *Risk Assessment and Management: a Complete Guide | British Safety Council*. [online] British Safety Council. Available at: https://www.britsafe.org/training-and-learning/informational-resources/risk-assessments-what-they-are-why-they-re-important-and-how-to-complete-them.
- Graves, R. (2000). *Qualitative risk assessment*. [online] Pmi.org. Available at: https://www.pmi.org/learning/library/qualitative-risk-assessment-cheaper-faster-3188.

- Safran (2022). *An Introduction to Qualitative Risk Analysis | Safran*. [online] www.safran.com. Available at: https://www.safran.com/content/introduction-qualitative-risk-analysis.
- Evrin, V. (2021). *Qualitative vs. Quantitative Risk Assessment*. [online] ISACA. Available at: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/qualitative-vs-quantitative-risk-assessment.
- Gonzalez, Z. (2023). *Qualitative Risk Analysis & Quantitative Risk Analysis*. [online] SafetyCulture. Available at: https://safetyculture.com/topics/qualitative-and-quantitative-risk-analysis/.
- Vige, W. (2022). *Tips to protect your business from risk*. [online] Asana. Available at: https://asana.com/resources/risk-mitigation.
- Wojno, R. (2022). *The importance of risk mitigation*. [online] monday.com Blog. Available at: https://monday.com/blog/project-management/risk-mitigation/.
- Simmons, D., Dauwe, R., Gowland, R., Gyenes, Z., King, A., Riedstra, D. & Schneiderbauer, S. (N.D.). *2.1 Qualitative and quantitative approaches to risk assessment*. [online] Available at: https://drmkc.jrc.ec.europa.eu/portals/0/Knowledge/ScienceforDRM/ch02/ch02_subch0201.pdf.
- SOG (2023). *Exploring the 5 Principles of Risk Assessment: In Detail*. [online] SynergenOG. Available at: https://synergenog.com/principles-of-risk-assessment/.
- Manpreet (2023). *Effective risk calculation method for your organization*. [online] Scrut Automation. Available at: https://www.scrut.io/post/best-risk-calculation-method [Accessed 25 Feb. 2024].
- Bonnie, E. & Leach, J. (2021). *Essential Guide to Security Frameworks & 14 Examples*. [online] Available at: https://secureframe.com/blog/security-frameworks.