NAVIGATE COMPLIANCE

COMPLIANCE RE-IMAGINED

CERTIFIED DIGITAL PRACTITIONER: GOVERNANCE, RISK AND COMPLIANCE

SAQA ID: 1303

Module 2: Risk Management

Table of Contents:

.....1

LEARNING OUTCOMES.....3

LEARNING OUTCOMES

By the end of this module, learners should be able to:

1. Define **risk** and explain how it includes both **threats and opportunities**.

2. List and describe the main **types of risk** with simple examples.

3. Explain the purpose of **risk management** in an organisation.

4. Understand and apply the **RAISE** process: Recognise, Analyse, Identify, Suggest, Evaluate.

5. Describe how **corporate governance** and risk management work together.

1. DEFINING RISK

Risk refers to the uncertainty surrounding future events and the possibility that outcomes may differ from what was planned or expected. This uncertainty can result in negative consequences, such as financial losses, operational disruptions, system failures, cyberattacks, reputational damage, or legal and regulatory penalties. At the same time, risk also includes the possibility of missed opportunities, where organisations fail to grow, innovate, or gain competitive advantage because they were too cautious or unprepared to act.

Risk is therefore not only about preventing harm, but also about recognising and managing uncertainty in a way that allows an organisation to benefit from positive possibilities. Every strategic decision carries some level of risk, whether it involves launching a new product, entering a new market, adopting emerging technology, or partnering with a new client segment.

While these actions may expose the organisation to potential losses or challenges, they also create opportunities for growth, efficiency, and innovation. An organisation that seeks to eliminate all risk entirely is likely to stagnate, fall behind competitors, and struggle to adapt in a rapidly changing environment.

Effective risk management does not mean avoiding risk, but rather understanding it, assessing its potential impact, and making informed decisions that balance risk and reward while protecting the organisation’s value, objectives, and long-term sustainability.

2. TYPES OF RISK

In organisations, risk comes in different forms. Below are common risk categories that leaders, managers and employees should understand.

2.1 Financial Risk – "The Cash Cruncher"

Financial risk refers to the possibility that an organisation's money, cash flow, profitability, or overall financial stability may be negatively affected. This type of risk often arises when clients fail to pay their accounts on time, interest rates increase unexpectedly and make loan repayments more expensive, or exchange rate movements drive up the cost of imported goods and services. If financial risk is not properly managed, an organisation may struggle to pay salaries or suppliers, experience sustained financial losses, or, in severe cases, face insolvency and business closure.

2.2 Operational Risk – "The Process Breaker"

Operational risk arises from failures or weaknesses in internal processes, people, systems, or from external events that disrupt normal day-to-day operations. Examples include system outages that delay deliveries, human error resulting in incorrect orders being shipped, or a key supplier suddenly shutting down and failing to deliver critical inputs. When operational risks are left unmanaged, organisations often experience service delays and backlogs, increased customer complaints and cancellations, and higher costs associated with correcting errors and restoring operations.

2.3 Cyber Risk – "The Invisible Hacker"

Cyber risk relates to threats affecting information systems, networks, data, and online services, particularly in an increasingly digital business environment. This may include employees falling victim to phishing emails that introduce malware into the network, customer data being stolen from online platforms, or ransomware attacks that encrypt company files and demand payment for their release. If cyber risks are not effectively managed, organisations may suffer the loss or theft of

sensitive information, face regulatory fines and legal claims, and experience serious reputational damage that erodes client trust.

2.4 Strategic Risk – "The Bad Decision"

Strategic risk occurs when an organisation's strategy, business model, or long-term direction is poorly aligned with its external environment. This can happen when significant resources are invested in products that customers no longer want, when emerging competitors, technologies, or market trends are ignored, or when expansion into new regions takes place without sufficient understanding of local conditions. Poorly managed strategic risk can result in loss of market share, wasted investments and resources, and the gradual long-term decline of the business.

2.5 Compliance Risk – "The Rule Breaker"

Compliance risk refers to the risk of failing to comply with applicable laws, regulations, industry standards, or internal policies and procedures. Common examples include non-compliance with data protection legislation such as POPIA or GDPR, failure to meet anti-money laundering (AML) obligations, or neglecting workplace health and safety requirements. When compliance risks are not managed effectively, organisations may face fines, penalties, and regulatory enforcement actions, loss of licences or authorisations, and in serious cases, criminal or civil liability.

2.6 Reputational Risk – "The Trust Breaker"

Reputational risk arises when stakeholders such as customers, employees, regulators, investors, and the public lose trust in the organisation. This may be triggered by social media scandals involving unethical behaviour or discrimination, poor handling of customer complaints that becomes public, or high-profile data breaches reported in the media. If reputational risks are not addressed, organisations may lose customers to competitors, struggle to attract and retain talented employees, and experience declining confidence from investors and business partners.

2.7 Environmental and Social Risk – "The Impact Ignorer"

Environmental and social risk stems from the organisation's impact on the environment and

broader society. Examples include pollution that harms surrounding communities, unsafe working conditions or unfair labour practices, and projects that damage ecosystems or displace local populations. When these risks are not properly managed, organisations may face community protests and boycotts, negative media coverage and campaigns by non-governmental organisations, as well as regulatory sanctions and the loss of their social licence to operate.

2.8 Summary Table – Types of Risk

Type of Risk	Main Focus	Simple Example
Financial	Money & profits	Client does not pay → cash flow problem
Operational	Processes & systems	System failure → delivery delays
Cyber	Data & IT systems	Phishing attack → data exposed
Strategic	Direction & strategy	Launching a product nobody wants
Compliance	Laws & regulations	Ignoring POPIA → possible fine
Reputational	Brand & trust	Scandal trending on social media
Environmental & Social	Society & environment	Factory pollution → protests and penalties

3. WHAT IS RISK MANAGEMENT?

Risk management is the process of:

1. **Identifying** risks,
2. **Assessing** how serious they are,

3. **Deciding** what to do about them, and
4. **Monitoring** them over time.

Risk management is not about avoiding all risks. It is about **making informed decisions**, protecting value and enabling performance and innovation.

3.1 Why Risk Management Matters

Effective risk management helps organisations to:

- Reduce the likelihood and impact of negative events.
- Protect their financial health, data and reputation.
- Comply with laws and regulations.
- Make better strategic decisions.
- Improve resilience in a changing environment.

4. THE "RAISE" RISK MANAGEMENT PROCESS

A simple way to remember the risk management steps is the acronym **RAISE**:

1. **Recognise the Risk**
2. **Analyse the Impact**
3. **Identify Controls**
4. **Suggest Risk Treatment**
5. **Evaluate and Monitor**

Step 1: Recognise the Risk

The first step in managing risk is recognising that it exists and understanding where it may arise. This involves asking simple but important questions such as what could go wrong in our daily operations, decisions, or projects, what opportunities we might miss if we do nothing, and what has gone wrong in the past.

For example, a business launching an online payment system should consider the risk of system outages, fraud, or customers abandoning the platform due to poor user experience. Recognising risk is not a one-person exercise and works best when different teams are involved, as each team sees risks from a different angle.

Organisations can identify risks by brainstorming together, reviewing past incidents, customer complaints, audit findings, and near-misses, and paying attention to warning signs. It is also important to stay aware of changes outside the organisation, such as new laws or regulations, emerging technologies, shifts in customer behaviour, actions by competitors, or social and environmental expectations. By actively looking for risks instead of waiting for problems to happen, organisations can prepare early and make better, more informed decisions.

Ask:

- What could go wrong?
- What could we miss out on?
- What has gone wrong before?

Let's look at how these different risks can be identified in practice using the examples below.

Financial Risk

A small business relies heavily on one major client, and that client delays payment by 60 days, putting pressure on cash flow. Another example is when interest rates rise unexpectedly,

increasing loan repayments and reducing monthly profits. Currency fluctuations can also increase costs when a business imports goods or software priced in foreign currency.

Financial risks are usually identified by reviewing budgets, cash-flow statements, management accounts, and payment trends. Warning signs include late-paying customers, declining profit margins, rising debt levels, or increasing costs. These risks are assessed by asking how likely cash shortages, losses, or cost increases are, and how serious the impact would be on salaries, suppliers, and operations. Financial risks are managed by actions such as diversifying the client base, setting credit limits, improving debtor collections, maintaining cash reserves, hedging foreign exchange exposure, and regularly reviewing financial forecasts.

Operational Risk

An organisation's IT system crashes on a busy day, delaying customer orders and service delivery. A staff member enters incorrect data, resulting in invoices being sent to the wrong customers. A supplier suddenly goes out of business, leaving the organisation without critical materials needed to operate.

Operational risks are identified by looking at how daily processes work in practice. This includes reviewing incident logs, customer complaints, audit findings, system downtime reports, and staff feedback. For example, repeated delivery delays or frequent system errors signal operational weaknesses. These risks are assessed by considering how often disruptions occur and how badly they affect service delivery and costs. Management responses may include improving processes, training staff, introducing quality checks, strengthening supplier agreements, and implementing backup systems or contingency plans.

Cyber Risk

An employee clicks on a fake email that looks legitimate, allowing malware to enter the company network. Customer personal information is stored without proper security and gets accessed by

hackers. A ransomware attack locks access to company files, stopping operations until systems are restored.

Cyber risks are identified through IT risk assessments, vulnerability scans, penetration testing, audit reports, and monitoring security incidents such as phishing attempts or unauthorised access. The likelihood is assessed by looking at how exposed systems are and how often attacks occur, while impact is measured by the potential loss of data, business disruption, regulatory fines, and reputational damage. Cyber risks are managed through security controls such as firewalls, encryption, access controls, staff awareness training, incident response plans, regular system updates, and data backup and recovery processes.

Compliance Risk

The organisation fails to update its policies to comply with new data protection laws, leading to regulatory penalties. Required AML checks are skipped due to time pressure, exposing the business to enforcement action. Health and safety rules are not followed, resulting in workplace injuries and inspections.

Compliance risks are identified by tracking legal and regulatory requirements, reviewing policies and procedures, conducting compliance monitoring, and analysing audit or regulator findings. Changes in laws, such as data protection or AML regulations, often introduce new risks. These risks are assessed based on how likely non-compliance is and the severity of penalties, licence loss, or legal action. Management includes updating policies, training staff, appointing responsible officers, implementing compliance monitoring programmes, and engaging with regulators proactively.

Strategic Risk

A company invests heavily in a product that customers no longer want because market trends were ignored. Management delays adopting digital tools while competitors move ahead, causing loss of

market share. The business expands into a new country without understanding local regulations or customer behaviour.

Strategic risks are identified through strategic planning sessions, market research, competitor analysis, and environmental scanning. Signals include declining market share, changing customer behaviour, new technologies, or emerging competitors. Strategic risks are assessed by evaluating how likely a strategy is to fail and the long-term impact on growth, profitability, and sustainability. These risks are managed by regularly reviewing strategy, testing assumptions, diversifying offerings, investing in innovation, and ensuring leadership remains informed and adaptable.

Reputational Risk

A customer complaint goes viral on social media because it was handled poorly. A data breach is reported in the media, damaging public trust. Employees speak out publicly about unfair treatment, harming the organisation's brand and credibility.

Reputational risks are identified by monitoring customer feedback, social media activity, employee surveys, media coverage, and stakeholder engagement. A pattern of complaints, negative publicity, or internal culture issues can indicate growing reputational risk. These risks are assessed by considering how quickly trust could be lost and how difficult it would be to rebuild. Management actions include strong ethical leadership, clear communication, effective complaint handling, crisis management plans, and consistent alignment between values, behaviour, and public messaging.

Environmental and Social Risk

Operations cause pollution that affects nearby communities, leading to protests. Workers are exposed to unsafe conditions, resulting in injuries and public criticism. A development project harms local ecosystems, attracting attention from regulators and advocacy groups. These risks are identified through environmental impact assessments, workplace inspections, community engagement, and ESG reviews. Complaints from communities, safety incidents, or NGO attention often highlight these risks. They are assessed by looking at the likelihood of harm to people or the environment and the severity of regulatory, legal, and reputational consequences. These risks are

managed through responsible business practices, safety programmes, environmental controls, fair labour practices, sustainability initiatives, and ongoing engagement with affected stakeholders.

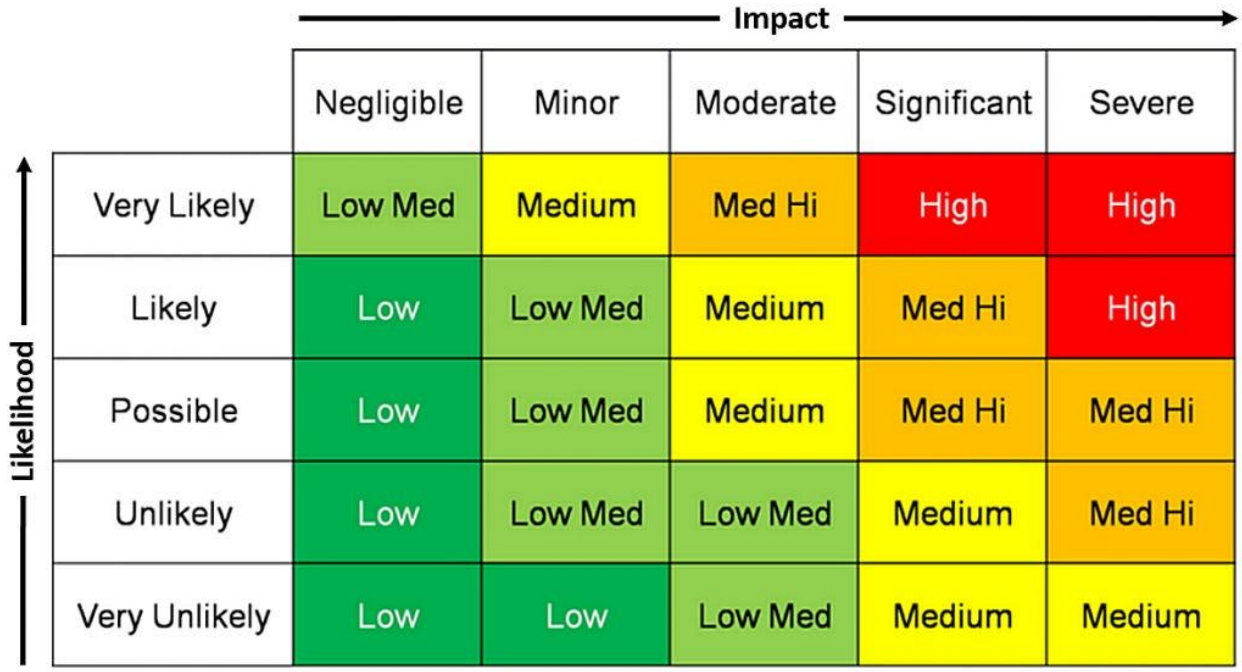
Together, these steps show that effective risk management is a **continuous cycle**. Risks are identified early, assessed realistically, and managed through practical controls and decisions. This approach allows organisations not only to protect themselves from harm, but also to operate responsibly, build resilience, and take informed risks that support long-term success.

Step 2: Analyse the Impact

Step 2 focuses on analysing the impact of each identified risk so that the organisation understands which risks require the most attention. **This step involves asking how likely (likelihood) it is that the risk will occur and how serious the consequences would be if it did happen (impact).**

For example, a minor system error that happens occasionally and is easy to fix may be less important than a cyberattack that is highly likely and could shut down operations or expose customer data.

A common way to analyse risk is by using a **likelihood vs impact scale**, often shown as a simple risk matrix or heat map. One side of the scale measures **likelihood**, ranging from *rare* to *almost certain*, while the other measures **impact**, ranging from *low* to *critical*. Each risk is placed on the matrix based on how often it might occur and how serious the consequences would be.



For example, consider the risk of an employee accidentally clicking on a phishing email. The likelihood may be rated as *likely* because phishing emails are common, and staff may not always spot them. The impact could be rated as *high* if it leads to a data breach or system downtime. When plotted on the matrix, this risk would fall into a high-priority zone, signalling that management action is required.

By contrast, a risk such as a brief power outage in an area with reliable backup systems might be rated as *possible* with a *low* impact. This would place it in a lower-priority area of the matrix. The visual scale helps organisations quickly see which risks need immediate attention, which should be monitored, and which can be accepted, ensuring that effort and resources are focused on what matters most.

Step 3: Risk Controls

Identifying controls involves understanding what measures are already in place to manage or reduce a specific risk. At this stage, organisations ask what they are currently doing to prevent the risk from occurring, to detect if it does occur, and to respond effectively afterwards.

Controls can take many forms. These include policies and procedures such as KYC processes, approval limits, segregation of duties, and documented workflows that guide how tasks should be performed. Controls also include systems and technology, for example firewalls to protect networks, data backups to prevent information loss, access controls, and CCTV to monitor physical premises. People-based controls are equally important and include staff induction, ongoing training such as AML or cyber awareness programmes, and clear roles and responsibilities.

Controls generally fall into three categories: **preventative controls**, which are designed to stop a risk event from happening in the first place; **detective controls**, which help identify when something has gone wrong; and **corrective controls**, which focus on fixing the issue and reducing its impact after it has occurred. Understanding existing controls allows organisations to see what is working well, where gaps exist, and what additional measures may be needed to manage risk effectively.

Step 4: Suggest Risk Treatment

This means deciding what action should be taken to deal with a specific risk, based on its likelihood, impact, and the organisation's risk appetite. Once a risk has been identified and assessed, management must choose the most appropriate response rather than leaving the risk unmanaged. This involves considering whether the risk should be treated by putting stronger controls in place, transferred to another party such as through insurance or outsourcing, tolerated if the risk is low and acceptable, or terminated by stopping the activity that creates the risk altogether.

Effective risk treatment is practical and proportionate. For example, a high cyber risk may be treated by improving security controls and staff training, while a financial risk linked to rare events may be transferred through insurance. Low-impact risks may be tolerated but monitored, while

activities that pose unacceptable legal or reputational risk may need to be terminated. The aim of suggesting risk treatment is to ensure that risks are addressed in a deliberate, informed way that protects the organisation while still allowing it to operate and grow.

Common treatment options:

1. **Terminate or Avoid the risk**
    - Stop or do not start the activity that creates the risk.
    - Example: Not offering a product in a very unstable region.
2. **Treat or Reduce (mitigate) the risk**
    - Put controls in place to lower the likelihood or impact.
    - Example: Extra approval steps, system alerts, training.
3. **Transfer the risk**
    - Share the risk with another party.
    - Example: Insurance; outsourcing with clear contracts and SLAs.
4. **Tolerate or accept the risk**
    - Decide to live with the risk, but with awareness and monitoring.
    - Example: Low-risk issues where control costs are higher than the risk.

Step 5: Evaluate and Monitor Risks

Evaluating and monitoring risk is an ongoing process because risk is dynamic and constantly changing as the organisation, its environment, and external conditions evolve. New risks can emerge, and existing risks can increase, decrease, or change in nature over time.

For this reason, risk management does not end once controls are put in place. Organisations monitor risk through regular risk reviews and by keeping the risk register up to date, conducting

internal audits and testing the effectiveness of controls, and tracking incidents, near misses, and losses to identify patterns or weaknesses.

Risk information is also reported to senior management and boards to support oversight and decision-making. The purpose of evaluation and monitoring is to confirm that controls are **working as intended and that risks remain within the organisation's approved risk appetite.** Where controls are no longer effective or risk levels increase, corrective action can be taken early to prevent larger problems from occurring.

5. CORPORATE GOVERNANCE AND RISK MANAGEMENT

Corporate governance is the system of rules, processes, and structures through which an organisation is directed, controlled, and held accountable. It plays a critical role in ensuring that decisions are made responsibly, transparently, and in the best interests of stakeholders. Good governance and effective risk management are closely connected. Governance establishes who has the authority to make decisions, how those decisions should be made, and which frameworks, policies, and standards must be followed. Risk management, in turn, provides decision-makers with clear information about what could go wrong, how severe the potential consequences might be, and whether existing controls are working as intended.

Strong governance supports risk management through active leadership and board oversight. Leaders and boards set the tone from the top by promoting ethical behaviour, accountability, and risk awareness across the organisation. They approve risk management policies, frameworks, and risk appetite statements, and ensure these are aligned with the organisation's strategy and objectives. Regular risk reporting enables them to monitor key risks, challenge assumptions, and ask informed questions about emerging threats and opportunities. This level of oversight ensures that risk management is not treated as a tick-box or compliance exercise, but is embedded into strategic planning, performance management, and everyday decision-making. As a result,

governance and risk management together help protect organisational value, support resilience, and enable long-term sustainability

6. CASE STUDIES

The following real-world examples show what can happen when risks are not properly managed, and what organisations can learn from them.

Case Study 1: Equifax Data Breach (2017) – Cyber, Compliance and Reputational Risk

Background:
Equifax, one of the largest credit reporting agencies in the world, suffered a major cyberattack in 2017. Hackers accessed sensitive personal and financial data (including ID numbers and addresses) of around 147 million people in the United States and other countries.

Risks involved:

- **Cyber risk:** Vulnerabilities in systems were not patched in time.
- **Compliance risk:** Failure to adequately protect personal data.
- **Reputational risk:** Loss of public trust and intense media scrutiny.

Consequences:

- Regulatory investigations and legal action.
- Settlement amounts running into hundreds of millions of dollars.
- Severe damage to Equifax's reputation and brand.

Key lessons:

- Organisations must maintain strong cybersecurity practices, including regular patching and vulnerability management.
- Data protection and privacy obligations need to be taken seriously.

- Transparent and timely communication with customers after a breach is critical to managing reputational damage.

Case Study 2: Steinhoff Accounting Scandal (2017) – Financial, Strategic and Reputational Risk

Background:
Steinhoff International, a multi-national retail holding company with roots in South Africa, faced a massive accounting scandal in 2017. Irregular accounting practices overstated profits and assets over several years, leading to a dramatic collapse in its share price when the issues became public.

Risks involved:

- **Financial risk:** Misstated financial statements masked the true financial position.
- **Strategic risk:** Aggressive acquisitions and expansion without adequate controls and oversight.
- **Reputational risk:** Loss of investor confidence and public trust.

Consequences:

- Billions of rand in shareholder value were wiped out as the share price collapsed.
- Multiple investigations, lawsuits and settlements.
- Resignations of senior leadership and long-term damage to the Steinhoff brand.

Key lessons:

- Strong financial controls, audit functions and ethical leadership are essential.
- Boards must actively challenge management and understand complex transactions.
- Transparency and integrity in financial reporting are critical to sustaining trust.

Case Study 3: Boeing 737 MAX Crises (2018–2019) – Safety, Operational and Reputational Risk

Background:

Two fatal crashes involving the Boeing 737 MAX aircraft occurred in 2018 and 2019, leading to the deaths of 346 people. Investigations highlighted issues related to aircraft design, software (MCAS system), training and certification processes.

Risks involved:

- **Safety and operational risk:** Technical and design issues impacted safe operation of the aircraft.
- **Compliance risk:** Questions raised about regulatory approval and oversight.
- **Reputational risk:** Trust in Boeing's brand and commitment to safety was severely affected.

Consequences:

- Global grounding of the 737 MAX fleet for nearly two years.
- Significant financial losses due to cancellations, compensation and redesign.
- Long-lasting impact on Boeing's reputation among airlines, regulators and passengers.

Key lessons:

- Safety must always be prioritised over speed-to-market or cost savings.
- Robust risk assessments, testing and independent review are essential for critical systems.
- Organisational culture should encourage reporting of concerns rather than hiding issues.

Case Study 4: Cambridge Analytica and Facebook (2018) – Privacy, Compliance and Reputational Risk

Background:

In 2018, it emerged that data analytics firm Cambridge Analytica had improperly obtained data from millions of Facebook users, which was allegedly used for political advertising and profiling. This raised serious questions about privacy, consent and the use of personal data by digital platforms.

Risks involved:

- **Privacy and compliance risk:** User data was accessed and used in ways that many users did not clearly consent to.
- **Reputational risk:** Facebook faced widespread criticism from users, regulators and the media.
- **Strategic risk:** Dependence on data-driven advertising raised ethical and legal concerns.

Consequences:

- Regulatory investigations, including large fines and settlements.
- Damage to Facebook's public image and increased calls for stricter regulation of social media.
- Changes to privacy settings and data access for third-party apps.

Key lessons:

- Organisations must be transparent about how they collect, use and share personal data.

- Strong governance is needed over third-party access to systems and information.
- Ethical considerations around data use are as important as legal compliance.

---

7. SCENARIO PRACTICE

Use this scenario to practise applying the RAISE process.

Scenario: Logistics Start-Up

Zanele runs a small logistics company delivering goods across the country. She has just signed a contract to deliver medical supplies to several hospitals.

Suddenly, the following issues arise:

- One of her main delivery trucks breaks down.
- A driver's professional driving permit (PrDP) has expired.
- News reports warn of cyberattacks targeting GPS tracking systems used by logistics companies.

Questions:

1. Identify at least **three risks** in this scenario and classify them (financial, operational, compliance, cyber, reputational, etc.).
2. For each risk, suggest one **risk treatment option** using the RAISE approach.
3. Describe the potential impact on patients, hospitals and the business if the risks are not managed.

---

8. KNOWLEDGE CHECK – SELF-TEST QUESTIONS

Use these to revise before your assessment.

8.1 Multiple Choice

1. The main goal of risk management is to:
   A. Avoid all risks
   B. Manage uncertainty and protect business value
   C. Increase profits at all costs
   D. Outsource all difficult decisions

2. Which of the following is an example of **operational risk**?
   A. A share price collapse
   B. A system outage that delays customer orders
   C. A competitor entering the market
   D. A change in interest rates

3. Which risk treatment involves **sharing the financial impact** with another party?
   A. Avoid
   B. Reduce
   C. Transfer
   D. Accept

4. Reputational risk primarily affects:
   A. Cash flow only
   B. Systems and networks only

C. Stakeholder trust and brand image

D. Inventory levels

5. The “tone from the top” refers to:

   A. The CEO’s pay and benefits

   B. The organisation’s vision and mission statements only

   C. The example set by leaders on ethics, risk and compliance

   D. The layout of board reports

9. QUICK REVISION SUMMARY

Before writing your assessment for Module 2, make sure you can:

- Define **risk** and explain how it includes both **threats and opportunities**.
- List and describe the main **types of risk** with simple examples.
- Explain the purpose of **risk management** in an organisation.
- Understand and apply the **RAISE** process: Recognise, Analyse, Identify, Suggest, Evaluate.
- Describe how **corporate governance** and risk management work together.
- Learn from real-world **case studies** where risks became reality.
- Apply concepts to **scenarios** similar to the ones in this guide.