

## Part Two – Chartered Governance Qualifying Programme

# Risk Management

### Sample Marking Scheme

**Time allowed:** 3 hours (plus 15 minutes reading time)

**You must not take this paper out of the examination workspace.**

The examination paper contains **6** questions of which you must attempt **4**. You must attempt **3 questions** in Section A and **1 question** in Section B. The questions in Section A are based on the pre-released case study whereas the questions in Section B are not based on the pre-released case study.

Each question is allocated 25 marks. There are **100 marks** available in total for the paper.

**Note:** Unless otherwise specified, you should assume that an Act or an organisation referred to in the question is a UK Act or organisation.

---

# Pre-released case study

## Background

RichGold is a gold mining company which was established in June 2022 following the merger of Richard Mining (Rich) and GoldenMining (Gold).

Rich was mainly operated out of South Africa and Europe with their headquarters in London, England, whereas Gold's main operations were in North America with their headquarters in Denver, Colorado, USA.

The mining industry is one of the most heavily regulated and capital-intensive industries in the world, also facing particular challenges lately due to the heightened environmental awareness amongst the public and regulators. Mining companies are large risk-laden industrial enterprises that are managed through many difficult situations, including industry commodity price cycles, declining mineral reserves, and, usually operations in different jurisdictions often with poorly developed infrastructures.

In recent years, the mining industry has changed dramatically to improve processes, operations, working conditions and health, safety and environmental measures – at least for many enterprises. Mining can be a labour-intensive and unsafe occupation, although innovative techniques and equipment are now being applied in various areas of the industry to bring about improvements.

In addition, mining companies are being forced to modernise themselves to remain attuned to rapidly changing demands and expectations of their stakeholders. For example, the requirement to become sustainable by taking into consideration the planet, people and prosperity rather than just pure profit, whilst at the same time managing the bottom-line costs and delivering the above market average return to their investors. Rich had been slow in responding to these changes, not recognising their strategic value, as they had always made, what they felt was, a reasonable profit.

The merger between Rich and Gold allowed both companies to gain access to greater regional growth, economies of scale and also to build upon their strengths in health and safety (Gold) and project management (Rich).

The merged entity's corporate headquarters is located in London, England. RichGold was listed on the main market of the London Stock Exchange in February 2022, quickly being promoted the FTSE 100 index six months later. The first year of operating as a merged company produced a revenue of GBP 4.6 billion and a profit of GBP 1.1 billion. The profit was less than the combined profits of Rich and Gold in the previous year, but it did include the one-off merger related costs.

The new, combined workforce at RichGold is highly fragmented, driven by the different activities they undertake, their languages and geographies, the employment legislation and practices they comply with and their different corporate cultures. Some of the merger-related changes being undertaken have affected production targets and led to top talent being lost to competitors.

To further capitalise on the merger and in a bid to better reflect and respond to expectations from its stakeholders, the Board of RichGold want to improve their operational targets and business practices, including governance and risk management.

## Governance

The former Chief Executive Officer (CEO) of Gold, was a risk averse individual, (unusual for his industry), with a low risk appetite. He was opposed to the merger with Rich, considering the company to be too risk seeking, stating it would be 'Taking a risk too far'. He resigned as soon as the merger papers were signed.

In order to implement the merger and to achieve the merger's targeted market and improvement opportunities, RichGold hired a new CEO from a similar sized mining organisation, although with experience in the primary extraction of copper and silver rather than gold.

In fact, the CEO's brief specified that RichGold needed to be 'pulled into shape', using the merger as a chance to move forward and seize more opportunities in the growing market for gold.

The new Board of RichGold consists of two of the previous board members from Rich, two of the previous board members from Gold, and three new independent non-executive directors (iNed), one of whom is the new Chair of the Board.

There have also been major structural changes in the Executive Committee (ExCo), including the former CEO of Rich now being the deputy Chief Operating Officer (COO).

RichGold's current Board structure is shown below:

- Five Executive Directors:
  - Chief Executive Officer (CEO) - Alistair Gordon
  - Chief Financial Officer (CFO)
  - Chief Legal Officer (CLO)
  - Chief Operating Officer (COO) - Sanjay Busa
  - Chief People Officer (CPO) (appointed in March 2023) - Suchitra Abang
- Seven iNeds (appointed in January 2022 unless otherwise stated)
  - Chair of the Board and the Nominations Committee (new) – Katie Birchwood
  - Senior iNed (Gold) - Luke Sutcliffe
  - Chair of the Remuneration Committee (Rich)
  - Chair of the Audit and Risk Committee (new - appointed in December 2022) - Louis Mbappe
  - Three further iNeds: one new; one from Gold, and; one from Rich

The (ExCo) also includes the Health and Safety Director, the Development Director and the Technical Director.

To facilitate the transition of the newly merged entity, Board meetings take place every six weeks, preceded and informed by Board Committee meetings (Nominations, Remuneration, and Audit and Risk) and two weekly ExCo meetings. The meeting intervals are expected to become less frequent in 2024.

You are the new Company Secretary at RichGold, moving from the same role in an Oil and Gas extractive company at the time of the merger.

## **Risk and control**

Alistair and Sanjay are keen to move RichGold forward and develop initiatives to bring about the improvements outlined by the Board. As such, a new Chief Risk Officer (CRO) was hired in February 2022, who reports directly to Alistair.

During the due diligence exercise, it was discovered that Gold had focused their risk management approach entirely on the UK health and safety requirements (UK Health and Safety at Work Act). This approach was mirrored in the risk averse nature of the previous CEO of Gold.

Conversely, it was found that Rich was using its project risk management process to support decision making at strategic and business level. Although project risk management encouraged Rich to identify and manage both threats and opportunities, this approach no longer suits the business and governance requirements of the merged organisation.

Unfortunately, these focused approaches to risk management (health and safety and project management) have led to a lack of acknowledgement and management of some key strategic risks facing the organisation. Both companies managed to survive and be successful in this volatile industry, but the narrow focus of both approaches, and the low-risk appetite in Gold led to missed opportunities.

These missed opportunities impacted the development and expansion in the industry of both organisations. In addition, their focus meant that they did not recognise potential improvements in their internal governance, control and risk management approaches that would be considered best practice.

Following a recent audit at two of the operating sites, one in North America and another in South Africa, Louis has become concerned about the strength of the risk and control environment being implemented across the organisation. His concern centres not so much on the lack of controls in certain areas, but rather that he felt significant risks were not being identified or appropriately escalated and that some, more insignificant, risks were being over controlled. As such, he felt that there was an imbalance between the correct identification and prioritisation of risks and the associated controls applied.

Louis raised these concerns at the last Board meeting. He also expressed his worry that the Board were not constructively challenging the findings of audit reports or questioning the ExCo on whether RichGold was effectively identifying, managing and controlling its risks.

The board members from the original companies, Rich and Gold, did not receive these concerns well, considering the matters raised as a personal attack. They asked for it to be minuted that they did not appreciate being told that they were not doing their job effectively or that they were, in some way, negligent in their duties.

In the same meeting, Suchitra raised a significant concern about the negative impact the merger and various change management initiatives are having on the organisational human capital.

Again, some of the board members argued that a lot of planning had been done to consider the effect of these changes on the workforce to ensure staff remained engaged, reassured and motivated. It was noted that they had seen no evidence of any issues with RichGold's human capital, with Luke throwing up his hands and asking, 'What's your problem?!'.

At that point, Katie intervened to soothe the discontent in the meeting, and, in support of Louis, explained that as a newly merged organisation there were bound to be areas to be reviewed and that all the board members needed to grow and learn together to achieve the objectives of RichGold.

Katie suggested that they close the meeting at that point, and reserve time at the next Board 'off-site' session to consider these matters further when more research had been undertaken.

Suchitra had a brief discussion with you and Katie following the meeting, pointing out that she had found evidence of issues with the workforce, but did not have time to explain it at the board meeting. She noted the increasing turbulence in the staff turnover, highlighting problems in both recruiting and retaining key talent for the organisation.

In addition, Suchitra had found that workplace and management training has not been consistent or embedded across the organisation, nor have there been any staff surveys undertaken since the merger. Finally, personnel and skills-based analysis has not progressed further than the initial plan undertaken in September 2022.

Following the Board meeting and these brief discussions, you have some ideas on topics to include in the next 'off-site' Board session, not least of which will be the output of a review of the governance and risk management arrangements across the organisation, which Louis has asked you and the new CRO to undertake.

# Section A

Questions 1 to 4 are related to the pre-released case study. Answer three out of four questions.

- 1 Gold had been implementing the UK’s health and safety approach and Rich had been using a project approach to risk management across their separate businesses. As such, RichGold is now facing a lack of consistency in its implementation of risk management and a potential lack of understanding of the key risks in both its strategy development and execution.

As a result, the CRO wants RichGold to implement ISO 31000 as the consistent approach to enterprise risk management for the newly merged entity.

You have been asked to write a report to the Board, evaluating at least **three** high-level differences between health and safety, project and enterprise risk management and why enterprise risk management would be more appropriate for RichGold.

As part of the evaluation, focus on the **three** key parts of the ISO 31000 standard in creating and protecting value, and, in particular, the steps of the risk management process itself.

(25 marks)

Question number	Indicative content
<p>1 25 marks</p>	<p>Answers should provide confidence to the markers that the candidate has understood and demonstrated their learning in relation to health and safety and project risk management. In addition, candidates are expected to provide a comparison between the health and safety, project and programme, and enterprise risk management processes, including three high-level differences between all three approaches and why enterprise risk management would be more appropriate for RichGold.</p> <p>Candidates are also expected to demonstrate that they understand the ISO 31000 standard, including the Principles, Framework and each step of the risk management Process. It is not expected that students include the full process steps for project risk management from the Study Text, but where they do only two additional marks can be awarded. The answer should be formatted as a paper for the Board and include clear links to the case study.</p> <p><b>Answers could include the following content:</b></p> <p><b>Health-and-safety risk management</b></p> <p>Most organisations in most countries are subject to health-and-safety regulation. Health-and-safety regulation exists to protect stakeholders from death, injury and ill health (whether physical or mental health). The key stakeholder groups that are protected are employees, customers and third parties. Third parties may include households living near an organisation and who may be affected by its activities, such as by noise, air or ground pollution.</p> <p>Health-and-safety regulation exists because the market-based incentives for appropriate levels of health-and-safety risk-management are generally thought to be insufficient. Workers or customers could, for example, incentivise health and safety activities by demanding higher wages or paying a lower price if they believe their health or safety to be at risk. However, market-based incentives can be ineffective because of asymmetric information and public-good problems.</p> <p>Health-and-safety regulations generally cover the following risk-management activities:</p>

- the identification and assessment of health-and-safety hazards, including determining who might be affected (employees, customers and so on) and how they might be affected (injury or ill-health);
- taking appropriate measures to control health-and-safety hazards to protect stakeholders from harm;
- recording health-and-safety incidents and reporting major incidents to the relevant regulatory agency; and
- implementing appropriate policies and procedures for all of the above.

Most countries manage their health-and-safety regulations via government-appointed agencies. These agencies draw their power from laws that enable them to:

- implement new rules and guidance on health-and-safety management processes or the control of specific hazards;
- supervise the health-and-safety management activities of organisations; and
- take enforcement action to address any non-compliance.

*Health and safety is a fundamental aspect of risk management in the mining industry, and rightly so. The focus of this approach is on hazards and risk relating to them, such as slips, trips and falls. As such, approach relates to the management of threats leading to harm, injury, death or ill health of people.*

*This approach does not consider the wider strategic, tactical or operational risks, both threats and opportunities to an organisation.*

#### The UK Health and Safety Executive

The HSE is an independent health-and-safety regulator that draws its powers from the Health and Safety at Work Act 1974. The Act gave the HSE its powers to create regulations, inspect health-and-safety practices in organisations and take enforcement action, such as issuing fines, where necessary.

The 1974 Act places expectations on employees and employers, but prime responsibility for providing a safe working environment rests with the employer – which means an organisation's management and directors. Employers are expected to ensure that employees are protected from hazards that may endanger their health and safety 'as far as reasonably practical'. This includes providing appropriate levels of protection against hazards including fire, 'slips, trips and falls', dangerous equipment, excessively long working hours, or undue workplace stress. In return, employees are expected to co-operate with the health and safety activities of their employers and to act responsibly to ensure that they do not endanger themselves or others.

The Act covers non-employees who may be at a place of work, including contractors, suppliers, customers and third parties.

In addition to its regulatory, inspection and, enforcement powers, the HSE issues a wide range of guidance documents, designed to help an organisation to improve its health-and-safety management practices. This guidance is topic and industry-based. Topics include:

- dealing with asbestos;
- workplace stress;
- working at height;
- completing risk assessments;
- preventing slips, trips and falls;
- occupational diseases; and
- dealing with noise, vibration, gas and electricity.
-

Industry-specific guidance covers sectors such as:

- nuclear power;
- fishing and farming;
- quarries;
- food;
- diving;
- tree work;
- cleaning; and
- the production and use of chemicals and explosives.

*Details of the UK Health and Safety at Work Act are not necessary for this answer, however, the information is provided for the markers should a candidate include details in their answer. No additional marks will be awarded for including details of the UK Health and Safety at Work Act.*

### **Project risk-management**

Project management is concerned with planning and co-ordinating the work of a team of people to achieve specific goals, within a specified time period, often with limited financial and human resources. Projects are temporary endeavours, but the changes that they bring may be permanent. Examples of projects within organisations include:

- designing and implementing a new IT system;
- moving or refurbishing a work site (office or factory);
- research and development of a new product or process;
- launching a new product;
- implementing new operational processes;
- merging with another organisation;
- implementing new risk-management or corporate-governance arrangements; and
- setting up a new subsidiary in a new location or market.

Multiple related projects may be grouped into a wider programme. For example, the implementation of a new risk management framework may have one project dealing with implementing a supporting IT system; another dealing with changes to governance arrangements; and further projects implementing new risk assessment and control and reporting arrangements.

All projects are conducted within a range of constraints, including financial, time and quality constraints. Projects can be complex, requiring the co-ordination of different resources, skills, knowledge and expertise, all of which is subject to a range of risks that may result in delays, cost overruns and poor quality implementation. Poor quality implementation can be especially problematic. For example:

- a new IT system may be unreliable or require extensive manual workarounds that negate any efficiency gains;
- a new location or refurbishment may prove to be unsuitable to employee needs (too hot, too cold, damp, lacking adequate light, noisy and so on);
- a new product or process may come with design flaws or prove to be unreliable;
- a merger may lead to culture clashes between the two organisations and fail;
- new risk-management and governance arrangements may not comply with relevant laws and regulations; and
- the products offered by a new subsidiary may not meet the needs of consumers.

Project risk-management ensures that project objectives are delivered on time and on budget. Project risk managers use a range of practices to identify, assess, monitor and control project risks to ensure the smooth progress of a project or programme.

*It is not expected that candidates include the steps of the project risk management process provided in the study text, however, the information is provided for the markers should a candidate include details in their answer. No additional marks will be awarded for the steps of the project management process.*

Ward provides a nine-phase process for managing risk within projects and programmes. This is summarised in the following Table:

Phase	Description	Objective
Define	Define the scope of the project and the project constraints, to avoid the risk of any misunderstanding.	Ensure that project participants have a shared understanding of the project and that all project information can be accessed quickly and easily between participants.
Focus	Focus on the agreed risk management objectives and processes.	Ensure that all participants understand the project objectives and that risk-management tools are established, within any cost or resource constraints.
Identify	Identify the threats and opportunities associated with the project.	Participants must understand the potential risks, the causes and effects to manage a project effectively.
Structure	Structure risks according to their type, severity of exposure, management expertise required and so on.	Ensure that risks are categorised by type to allow appropriate expertise to be focused on them. Structure risks by probability and impact to facilitate prioritisation.
Ownership	Assign risks to owners according to type and the severity of exposure.	Ensure that the right expertise is available to manage risks. Ensure that risks are escalated to the appropriate level of management, depending on their severity.
Estimate	Continue to estimate risk exposures to keep track of any changes.	Ensure that risks are monitored on a regular basis and that the results of this monitoring activity are reported.
Evaluate	Evaluation of project risk management activities.	Evaluate the effectiveness of project risk-management activities, including assessment and control activities.
Plan	Project plan and associated risk management plans.	All projects require careful planning, and plans may need to be revised in the light of risks or other unplanned factors. Risk-management plans ensure that mechanisms are in place to respond to changes in risk exposure or the emergence of risks during a project.
Manage	Management and control of the project through its lifetime.	Monitor project progress and manage any loss events or crises that occur.

The specific risk-management tools that are used within the project risk-management process are very similar to those for other types of risk. Common tools include risk registers, risk reports of key risk indicators (KRIs) and key performance indicators (KPIs), project risk committees and crisis management. Organisations may have specialist project risk managers, project-management specialists with a knowledge of risk-management, or risk-management

specialists that support project-management teams. External project-management specialists may be used for technical projects or in smaller organisations.

A formal methodology for managing projects, including the risks that are associated with projects, is known as PRINCE2 (PProjects IN Controlled Environments).

The PRINCE2 methodology builds risk-management into the management of a project from the beginning and should, if applied correctly, incorporate Ward's nine phases of project risk-management. Within the PRINCE2 approach, risks are captured on risk registers; issues and quality concerns are captured on issue registers and quality registers. Issue and quality registers may contain information on actual loss events as well as potential control issues. Lessons logs ensure that valuable learning experiences are not missed, so that project risks can be addressed more effectively in the future.

The Project Management Institute (PMI) is a professional institute for project managers, including experts in project risk-management. The PMI provides practice standards for project managers, including a practice standard on project risk-management.

As an alternative to PRINCE2, the Association for Project Management (APM) in the UK has developed the Project Risk Analysis and Management Method. The purpose of this method is to support identification, assessment, monitoring and control of project risks.

One advantage of the PRAM approach is that risk is recognised as both an opportunity and a threat.

*It is not expected that candidates include the different project risk management methodologies provided in the study text, however, the information is provided for the markers should a candidate include details in their answer. No additional marks will be awarded for the different methodologies, except in the recognition of risk as both an opportunity and a threat.*

*As noted in the case study, the project risk management approach includes the assessment and management of opportunities. This is a value adding aspect of the risk management process can be used at all levels of the business, but the focus on the temporary nature of projects, within cost, time and budget restrictions, is not appropriate for the ongoing operational and governance requirements of the organisation.*

### **ISO 31000 – Risk Management: Guidelines**

This ISO distinguishes between a risk-management framework, principles and process. However, this does not imply that these elements are independent. The principle and process elements feed into the framework element. A risk-management framework also includes risk-management principles and the risk-management process.

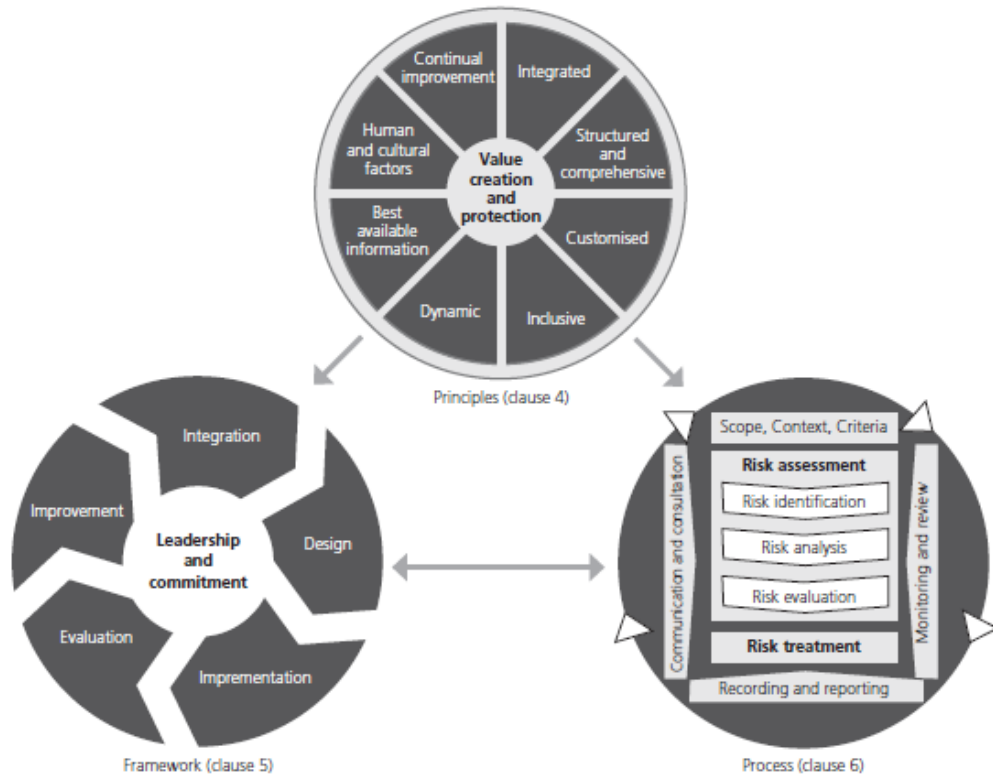
The ISO perspective is conceptual and so helps to avoid the confusion that can sometimes exist between these three elements. In practice, the term framework is used to refer to the variety of policies, procedures, processes and tools that comprise an organisation's risk-management activities. The purpose of these policies, processes and tools is to provide a coherent structure to support the management of risk within the organisation.

*This would support RichGold in putting forward a consistent approach to risk management across the organisation.*

This framework should ensure that the level of risk-taking within the organisation supports the achievement of its strategic objectives and is consistent with the risk preferences of its stakeholders. This will include taking potentially positive risks in order to exploit potential business opportunities, while at the same time attempting to prevent and mitigate more damaging risks, such as fraud, health-and-safety events, fires or pollution. The ultimate aim is to use the risk-management framework to add value to an organisation, helping it to operate in a successful and sustainable way over the long term.

*This enables RichGold to bring in both aspects of risk – threat and opportunity – but not restricted to a health and safety or project focus. It enables the organisation to consider risks across the merged entity, looking at the upsides and downsides.*

The ISO 31000 standard is illustrated in the diagram below.



The practice of risk-management took a major leap forward in 2009 when the ISO published ISO 31000. This, in turn, was updated in 2018 to reflect advances in practice and changes to certain risk exposures such as cyber risk and terrorism.

*This enables RichGold to bring in both aspects of risk – threat and opportunity – but not restricted to a health and safety or project focus. It enables the organisation to consider risks across the merged entity, looking at the upsides and downsides.*

The objective for ISO 31000 is to provide a set of internationally recognised principles and guidance on the practice of risk-management in organisations. These principles and guidance may be used to help improve the design and implementation of a risk-management framework within an organisation.

As with any international standard, ISO 31000 provides a universal benchmark for risk-management practice, helping an organisation to improve the effectiveness of its risk-management framework and related activities, irrespective of its market sector or business model. The standard does not promote a uniform approach to the practice of risk management but encourages organisations to adapt the principles in order to design and implement a risk-management framework that is consistent with the nature, scale and complexity of their activities.

*This concept supports an appropriate approach for RichGold. It recognises that the approach can be tailored to the complexities of the organisation, and that in doing so RichGold can still benchmark itself against an international standard.*

ISO 31000 covers a wide range of topics, including:

- definitions for key terms such as risk, uncertainty and risk-management;
- the importance of managing both the opportunities and threats that may come from exposure to risk;
- the basic principles for effective risk-management, such as developing a risk-aware culture, ensuring that it supports the organisation's strategic objectives and ensuring it is practised on a continuous basis to keep track of changing risks and exposures;
- how to design, implement, review and improve an effective risk-management framework; and
- the key components of an effective risk-management process for identifying, assessing, monitoring and controlling risk.

The 2018 update of the standard is more concise than the 2009 original. This is because a series of additional guidance documents are expected. Each will add further detail on the high-level content within the main ISO 31000 document.

The 2018 document is centred on three main topic areas:

1. principles for risk-management
2. core elements of an effective risk-management framework
3. the risk-management process.

*It is expected that candidates include the three main topic areas of the ISO standard – the principles, framework and also the process. The standard is not just a process.*

The core principle in the revised standard is that risk-management activity should help protect and create value in organisations. Value might be protected through the prevention of costly negative risk events. Value might be created by using risk-management to satisfy the expectations of stakeholders or to help an organisation fulfil its strategic objectives. Additional principles call for risk-management frameworks to be structured, inclusive, customised, dynamic and responsive, and integrated. This last principle, along with several of the others, is aligned to the practice known as enterprise risk-management.

*Candidates are expected to demonstrate their understanding of the principles, although it is not expected that they know all 8 principles or their details.*

In terms of designing an effective risk-management framework, the standard highlights how the external and internal context of an organisation will influence the design, implementation and ongoing review and improvement of the framework. External context means factors such as regulation, technological development and market forces. The internal context relates to factors such as the culture and structure of the organisation.

The standard emphasises the importance of leadership in designing and implementing effective risk-management frameworks. It argues that a tangible commitment to effective risk-management is needed from an organisation's leaders, including its managers, senior managers and board or equivalent. Support for an organisation's risk-management activities should be evidenced by what these leaders say and do. Leaders must communicate the importance of operating an effective framework and support this operation through their own actions.

*Candidates are expected to demonstrate their understanding of the framework, although it is not expected that they know all aspects of the framework.*

In terms of the risk-management process, the guidance discusses three core elements:

- establishing the context
- risk assessment

- risk treatment.

These are supported by three activities:

- communication and consultation
- recording and reporting
- monitoring and review.

*It is expected that candidates demonstrate their understanding of the process, including each step of the process as noted below.*

#### Establishing the context

Establishing the context includes understanding the internal and external drivers that may affect an organisation's exposure to risk, such as the physical environment, technology, organisational structures and processes. Context also means understanding the types of risk that may affect an organisation and the various assessment and control tools that are available for use. The aim is to ensure that the organisation understands the range and scope of its objectives and activities, and the risks that are associated with them.

#### Risk assessment

Risk assessment means that an organisation should identify, analyse and evaluate its exposure to all sources of risk to its objectives. Risk assessment may involve the use of statistical models or qualitative judgement.

#### Risk treatment

Risk treatment is another term for risk control. The aim is to ensure that the level of exposure is controlled: not too high or too low. The level of control will be influenced by the risk appetite of an organisation.

#### Communication and consultation

This is about communicating risk-management information (such as risk-management policies and procedures, or risk exposures) in a timely, accurate and factual way. Risk communication includes consulting with key stakeholders to ensure that they understand the risks that an organisation is taking and are satisfied that the organisation's approach to managing these risks is appropriate.

Communication seeks to promote awareness and understanding of risk and how to deal with it, whereas consultation involves obtaining feedback and information to support decision-making.

#### Recording and reporting

Recording means ensuring that identified risks are documented properly. It also means documenting risk-management processes and procedures to ensure that they are understood clearly and implemented coherently across the organisation.

Reporting means reporting on an organisation's risk exposures and the measures taken to control these exposures to relevant decision-makers and stakeholders.

#### Monitoring and review

Monitoring and reviewing is about learning, improving and adapting.

The performance of an organisation's risk-management framework can vary. If performance declines, changes may be required to maintain the efficiency and effectiveness of the framework. Performance monitoring and review might include activities such as audits, control effectiveness reviews and compliance reviews. ISO 31000 makes it clear that organisations should review and upgrade their risk-management activities on a regular basis. Risk, and an organisation's exposures to risk, are never static.

As an organisation changes its strategic objectives or operational activities, it must ensure that its risk-management framework and associated policies, processes, procedures and controls remain fit for purpose.

**Three differences between health and safety, project and enterprise risk management**

- *Health and safety and project risk management are focussed on particular areas and activities of the organisation, whereas enterprise risk management considers the whole risk profile across the organisation.*
- *Health and safety risk management considers threats only. This is often true of project risk management although opportunities do form part of this risk management process. Enterprise risk management considers both threats and opportunities.*
- *Enterprise risk management supports the achievement of an organisation's strategic objectives and is consistent with the risk preferences of its stakeholders, whereas health and safety and project risk management objectives are often set at lower, operational objectives and stakeholders in the organisation.*

*These or any other reasonable differences are acceptable.*

**Why enterprise risk management would be more appropriate for RichGold.**

*ERM considers risks across an organisation, looking at different aspects, rather than just health and safety or projects. This approach will enable the newly merged entity to better understand it's full profile of risks. In addition, the inclusion of opportunities, at both strategy development and implementation will support the Board in focusing on the appropriate risks. This will further support the effective control of risks, as the context and objectives will be better understood, and strategic risks will be recognised and managed according.*

*These or other reasonable reasons why ERM would be more appropriate for RichGold are acceptable.*

Level	Mark	Descriptor
	0	No rewardable material.
<b>Level 1 (Fail)</b>	1-12	<ul style="list-style-type: none"> <li>• The answer is not formatted as a Board report.</li> <li>• The answer gives an incomplete or incorrect understanding of health and safety and project risk management.</li> <li>• The answer provides an incomplete or incorrect comparison between the health and safety, project and enterprise risk management processes, with fewer than <b>three</b> high-level differences between all three approaches.</li> <li>• The answer provides incomplete or incorrect understanding of why enterprise risk management would be appropriate for RichGold.</li> <li>• The answer gives an incomplete or incorrect understanding of the ISO 31000 standard.</li> <li>• The answer provides an incomplete or incorrect information on the ISO 31000 Principles, Framework and each step of the Process.</li> </ul>

		<ul style="list-style-type: none"> <li>The answer makes few, if any, links between the theory and practice, using the case study.</li> </ul>
<b>Level 2 (Pass)</b>	13-16	<ul style="list-style-type: none"> <li>The answer makes some attempt to be formatted as a Board report.</li> <li>The answer provides a basic understanding of health and safety and project risk management.</li> <li>The answer provides a basic comparison between the health and safety, project and enterprise risk management processes, with <b>three</b> high-level differences between all three approaches.</li> <li>The answer provides an overview of why enterprise risk management would be appropriate for RichGold.</li> <li>The answer provides basic information on the ISO 31000 standard.</li> <li>The answer provides basic information on the ISO 31000 Principles, Framework and each step of the Process.</li> <li>The answer includes clear links between theory and practice, using the case study.</li> </ul>
<b>Level 3 (Merit / Distinction)</b>	17-25	<ul style="list-style-type: none"> <li>The answer is well formatted as a Board report.</li> <li>The answer gives a strong and comprehensive understanding of health and safety and project risk management.</li> <li>The answer illustrates a clear and comprehensive comparison between the health and safety, project and enterprise risk management processes, with <b>three</b> or more high-level differences between all three approaches.</li> <li>The answer gives a strong and comprehensive understanding of why enterprise risk management would be appropriate for RichGold.</li> <li>The answer illustrates a clear and strong understanding of the ISO 31000 standard.</li> <li>The answer illustrates a clear and comprehensive knowledge of the ISO 31000 Principles, Framework and each step of the Process.</li> <li>The answer makes strong links between theory and the case study, which is supported with appropriate examples both from the case study and the real world.</li> </ul>

- 2 It is clear that there is a lack of understanding of risk management, and corporate governance at all levels within RichGold. With the previous approaches being aligned to health and safety or project risk management, there has been more of a compliance or 'tick-box' attitude which has tended to be overly bureaucratic.

The new CRO, supported by Katie, Louis, Alistair and Sanjay, is keen to ensure that risk management is linked more to the development of strategy and acting on opportunities, as opposed to just mitigating threats and firefighting.

In your capacity as the Company Secretary, assess the relationship between risk management and corporate governance as part of the 'good' management of the company. Include in your assessment, an overview of the UK Corporate Governance Code, the link between risk management and strategy and the role of the Board in relation to strategy, risk management and corporate governance.

(25 marks)

Question number	Indicative content
<p>2 25 marks</p>	<p>Answers should provide confidence to the markers that the candidate has understood and demonstrated their learning in relation to role of risk management in an organisation its relationship to corporate governance as part of 'good' management. It is not expected that candidates provide excessive detail in any one part of this answer, as the time would not allow. However, the full information has been provided from the Study Text for the markers use in evaluating the answers provided.</p> <p>In addition, candidates are expected to provide an overview of the UK corporate governance code. Candidates are also expected to demonstrate that they understand the link between risk management and strategy and the role of the Board in relation to strategy, risk management and corporate governance. The answer should include clear links to the case study.</p> <p><b>Answers could include the following content:</b></p> <p><b>The relationship between risk management practices and corporate governance regulation as part of 'good' management</b></p> <p>Corporate governance is the system and related processes by which an organisation is directed and controlled. Effective corporate governance should ensure that an organisation is directed and controlled in a manner that meets the needs and expectations of its stakeholders. This can be achieved by setting strategic objectives that meet stakeholders' needs and expectations, as well as by implementing measures to identify, assess, monitor and control the various risks that could threaten the achievement of these objectives.</p> <p><i>It is not clear that the Board fully understand their role in relation to risk management as part of corporate governance. This would be an important aspect to make the Board aware of.</i></p> <p>One key link between corporate governance and risk-management is to identify and control the sources of risk that may either support or threaten the proper establishment and achievement of an organisation's objectives. A well-governed organisation should take all reasonable steps to ensure it determines the right activities to achieve its objectives effectively, efficiently and economically. The discipline of risk-management supports these activities with a range of tools and techniques that can be used to identify, assess, monitor, and ultimately control the risks to these objectives.</p>

These risks comprise the whole spectrum of uncertainty around the organisation's objectives, whether already chosen or still under consideration, and might include:

- risks that may affect the ability of an organisation to continue as a going concern, such as the establishment of a new form of subsidies, a large fraud or financial mismanagement;
- risks to the reputation of an organisation, such as the breakthrough of a new invention or a major scandal;
- risks which affect the continuity of the organisation's operations, such as the loss of a key outsource service provider; and
- other risks that may positively or adversely affect an organisation's objectives in relation to the non-financial needs of its stakeholders, such as ensuring their health and safety.

Good governance should effectively manage, not eliminate risk. Even a well-governed organisation may encounter risk events that threaten the achievement of its objectives. As the effects of risk can never be completely eliminated, organisations need to build both resilience and agility in all their activities, enabling them to adequately respond to changes in circumstances or to deal with the consequences of unforeseen events.

Another link between corporate governance and risk-management relates to the 'directed' element of corporate governance. For a board or senior management to appropriately determine the strategic objectives of an organisation, they will need to have a good understanding of the environment in which the organisation operates. They will also need to understand the capabilities of the organisation to function effectively within this environment and to exploit any opportunities that may be present. The environment will include a range of risks, including risks relating to customer demand, technology development or political change. It is up to the board and senior management to direct the strategy of the organisation in such a way that opportunities related to these risks can be exploited without unduly threatening its financial viability.

Good governance should ensure the long-term sustainability of an organisation, where value – for example, profits surpluses, environmental protection or some other social benefit – is generated through the exploitation of opportunities that contribute to the organisation's mission but which do not create an excessive level of risk or related financial failure, reputational damage or similar.

From a corporate governance perspective, the failure to exploit opportunities can be as destructive as a failure to manage the risks associated with opportunities that are exploited. The case of Kodak and the digital camera is a well-documented example of a failure to exploit a valuable opportunity.

The following quote from the UK Financial Reporting Council (FRC), the organisation tasked with overseeing UK corporate governance regulation, sums up these links between risk-management and corporate governance: 'Good stewardship by the board should not inhibit sensible risk-taking that is critical to growth. However, the assessment of risks as part of the normal business planning process should support better decision-taking, ensure that the board and management respond promptly to risks when they arise, and ensure that shareholders and other stakeholders are well informed about the principal risks and prospects of the company.' (FRC, 2014, p1).

*It is clear that risk management and corporate governance are interlinked, and that the good risk management and good governance can add value to the organisation, whether it is in exploiting opportunities or managing risks to ensure that strategic objectives can be achieved. As a mining organisation, with complex risks and increasing demands from stakeholders, understanding the context, the risks and appropriate controls, and being sustainable and resilient is all part of the 'good' management of the company.*

## Key risk-management regulations from the current UK Corporate Governance Code

The risk-management provisions contained within the UK Corporate Governance Code are as follows.

- The board is responsible for managing the principal risks an organisation is willing to take in the pursuit of its strategic objectives. The board is also responsible for ensuring that the organisation has sound risk-management and internal control systems. This should include mechanisms to monitor the soundness of these systems and reviewing the effectiveness of these systems at least annually.
- Non-executive directors should scrutinise management performance, including the robustness of the organisation's financial controls and risk-management systems.
- A board audit committee or a separate board risk committee should normally be in place to support the work of the board on internal control and risk-management.
- Information on the organisation's principal risks and the soundness of its risk-management and internal control systems should be provided in the annual report.
- The board's work on risk-management should include consideration of the organisation's appetite for risk, as well as embedding the desired culture and the related risk culture. The board should also consider the risks associated with strategic change and other major change initiatives, as well as the effectiveness of an organisation's crisis management and business continuity arrangements.

Principal risks are large-scale risks to the achievement of an organisation's strategic objectives that may threaten the business model, future performance, the solvency (capital and other financial resources) and liquidity (cash flows) of an organisation.

Board members clearly need to pay particular attention to these principal risks, but the UK Governance Code makes it clear that boards are responsible for overseeing the management of all risks. A board will usually delegate the management of tasks with fewer significant risks to lower management in the organisation.

*It is not expected that candidates include details of the history UK Corporate Governance Code and no additional marks will be awarded were it has been included. It is expected that students understand the concept of 'comply and sign', and have demonstrated that they understand that the Code has risk management provisions, without the need to detail those provisions. The details have been included for the information of the markers should a candidate include them.*

### **Linking risk to strategy**

There has been a growing demand for more effective risk-management practices to cope with the rapidly changing business environment, especially since the financial crisis of 2007–08. Many of these changes involve regulatory or industry-standard-related compliance that put organisations under great public and regulatory scrutiny, such as:

- anti-money laundering
- anti-terrorism financing
- climate change disclosures
- corporate governance reporting
- environmental compliance
- contingency planning
- data protection regulations
- Basel financial regulations.

As a result, many organisations are already incorporating the management of strategic risks within their overall risk management framework. However, the scope of strategic risk-management practices is often too narrow.

Many organisations focus on assessing and managing risks that arise from a chosen strategy or different components of a strategy. For example, a strategic risk-management framework often does not capture the preliminary step of assessing and categorising alternative strategies, nor does it capture the execution of a strategy risk or the assessment on how a chosen strategy supports organisational expertise, corporate mission and long-term objectives.

Expertise and mission alignment is particularly relevant when an organisation is pursuing a sizeable business acquisition. For example, one of the key reasons why Interserve plc (a UK-based construction company with over £3 billion of annual Risk Management revenues and 75,000 employees worldwide) faced a collapse in its share price throughout 2017–18, and a real risk of bankruptcy in 2019, is because of its ill-conceived strategic decision to expand into the energy-from-waste sector where it had no expertise (including risk-management expertise).

There remains a further need to strengthen the strategic-risk framework to better connect different decision-making steps, including:

- the initiation of a strategic review;
- the assessment of alternative strategies (including their overall fitness) •
- the execution of a strategy; and
- monitoring and managing risks that arise from a chosen strategy.

*The link between corporate governance and risk management has been made earlier. This relates mostly to the implementation of strategy for an organisation. What is considered here is how risk management can be used in setting strategic direction.*

#### The role of the board

Boards have undergone a considerable evolution in relation to their oversight of both risk and strategy, often including the appointment of senior executives responsible for managing these areas.

Boards are already responsible for formally approving the aggregate level of risk an organisation can take in pursuing its strategy, (the risk-appetite statement). They also set the strategy that must be reflective of the organisational values and behaviours (corporate culture).

As organisational strategies evolve, and business threats become more complex and frequent, bringing risk closer to strategy is the next logical step in order for boards to remain effective in their oversight of an organisation. However, many organisations still struggle when it comes to articulation of their aggregate risks and how they link to their strategy.

A more comprehensive understanding of non-financial risks that emanate from strategy is also an area that is still evolving. Many boards employ third-party experts to help them independently review different aspects of external threats, and understand how these threats may translate into actual losses for an organisation.

The advantages of linking risk to strategy are that it allows for a clearer assessment of aggregate risks related to a particular strategy, as well as enabling board-level discussions on whether alternative strategies present a more attractive risk/return choice for an organisation.

	<p>Overall, boards have been taking a more significant role in linking organisational risks to strategy, by incorporating new processes and behaviours:</p> <ul style="list-style-type: none"> <li>• Challenging management on key risk-appetite assumptions and definitions. Boards are expected to have a comprehensive understanding of the different risks that form the risk-appetite statement, and to treat risk as part of the decision-making process.</li> <li>• Seeking more comprehensive assurances from management on how the non-financial risks are monitored and mitigated versus a simple 'yes or no' approach. Boards are expected to ask management to quantify such risks in terms of their impact on the value of an organisation.</li> <li>• Encouraging management to discuss risks in relation to the strategy.</li> <li>• Hiring independent external advisors to evaluate risks of acquiring a sizable business or asset.</li> <li>• Connecting the internal audit function to strategic planning and strategic risk-management processes, as well as calibrating the output from the internal audit reports within the context of strategy.</li> </ul> <p>As stewards of an organisation, boards have an opportunity to expand their role beyond traditional risk oversight by providing strategic advisory guidance to management and helping them see the bigger picture.</p> <p><i>Louis has previously noted his concerns not just on the lack of controls in certain areas, but also that significant risks were not being identified or appropriately escalated, and that some risks were being overcontrolled. In addition, he noted his worry that the Board were not constructively challenging findings from audit reports or questioning the ExCo on the effectiveness of the risk management process. It would be appropriate to raise role of the Board in using risk management in strategy setting and challenging and questioning risk information.</i></p>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Level	Mark	Descriptor
	0	No rewardable material.
<b>Level (Fail)</b> 1	1-12	<ul style="list-style-type: none"> <li>• The answer provides an incomplete or incorrect understanding of the relationship between risk management and corporate governance as part of 'good' management.</li> <li>• The answer provides incomplete or incorrect understanding the UK Corporate Governance Code.</li> <li>• The answer gives an incomplete or incorrect understanding of the link between risk management and strategy.</li> <li>• The answer provides and incomplete or incorrect understanding of the role of the Board in relation to strategy, risk management and corporate governance.</li> <li>• The answer makes few, if any, links between the theory and practice, using the case study.</li> </ul>
<b>Level (Pass)</b> 2	13-16	<ul style="list-style-type: none"> <li>• The answer provides a basic understanding of the relationship between risk management and corporate governance as part of 'good' management.</li> <li>• The answer provides an overview the UK Corporate Governance Code.</li> <li>• The answer provides a basic understanding of the link between risk management and strategy.</li> </ul>

		<ul style="list-style-type: none"> <li>• The answer provides a basic understanding of the role of the Board in relation to strategy, risk management and corporate governance.</li> <li>• The answer includes clear links between theory and practice, using the case study.</li> </ul>
<b>Level 3 (Merit / Distinction)</b>	17-25	<ul style="list-style-type: none"> <li>• The answer gives a strong and comprehensive understanding of relationship between risk management and corporate governance as part of 'good' management.</li> <li>• The answer illustrates a clear and comprehensive understanding of the UK Corporate Governance Code.</li> <li>• The answer gives a strong and comprehensive understanding of the link between risk management and strategy.</li> <li>• The answer illustrates a clear and strong understanding of the role of the Board in relation to strategy, risk management and corporate governance.</li> <li>• The answer makes strong links between theory and the case study, which is supported with appropriate examples both from the case study and the real world.</li> </ul>

PILOT PAPER

3. The previous CEO of Gold had a low-risk appetite, looking to mitigate all threats at almost any cost with his cautious approach to risk management. While this has provided a very safe working environment, it has led to a number of business and work practice opportunities being overlooked.

There is a new remit from the Board to look for opportunities, with Alistair wanting to ensure the Board and ExCo understand 'how much risk is too much risk' – RichGold's risk appetite.

To support Alistair in introducing the concept of risk appetite at the next Board 'off-site' session, prepare a report which assesses risk appetite and risk tolerance in supporting risk-based decision making. As part of this report, include:

- the difference between risk appetite, risk tolerance and risk capacity
- how risk appetite can be used to support decision making and the maintenance of appropriate corporate governance
- how the Board might determine their risk appetite
- the Board's role in determining risk appetite.

(25 marks)

Question number	Indicative content
3 25 marks	<p>Answers should provide confidence to the markers that the candidate has understood and demonstrated their learning in relation to risk appetite, risk tolerance and risk capacity. It is not expected that candidates provide information on implementing or expressing risk appetite for the organisation. Where these aspects are included in the answer, an additional two marks, in total, can be awarded by the markers – the focus, however, should be on introducing risk appetite to the board.</p> <p>In addition, candidates are expected to demonstrate that they understand the role of risk appetite in supporting decision making and maintaining appropriate corporate governance. Candidates are also expected to demonstrate that they understand how the Board might determine their risk appetite and their role in doing so. The answer should be formatted as a paper for the Board and include clear links to the case study.</p> <p><b>Answers could include the following content:</b></p> <p><b>Risk appetite, risk tolerance and risk capacity</b></p> <p><u>Defining risk appetite</u></p> <p>There are many definitions of risk appetite within standards, regulations, documents from professional associations and academic research. Most fall into two perspectives:</p> <ul style="list-style-type: none"> <li>• definitions that define risk appetite in terms of the level of risk exposure that an organisation is prepared to accept; and</li> <li>• definitions that define risk appetite in terms of an organisation's willingness to take a defined level of risk in the pursuit of its strategic objectives.</li> </ul> <p>Definitions that focus on the acceptability of risk tend to focus on downside risks that may only result in losses. As it is impossible to eliminate risk completely, a degree of risk exposure must be accepted and an organisation's appetite for risk denotes the level of risk exposure that it is prepared to accept.</p> <p>Definitions that talk about a willingness to take risks recognise that exposure to risk can be good, as it can lead to positive outcomes. In this context, an organisation must</p>

determine the risks that yield the highest possible outcomes, while remembering that with the potential for large positive outcomes comes the potential for large negative ones.

An organisation must decide the level of risk exposure that provides an optimal balance between the upsides and downsides of risk-taking. Most organisations can only achieve their objectives if they take risks. Without risk there would be no opportunities to exploit, no products and services, and no returns to earn. The trick is to take the right risks and the right level of exposure to these risks. The concept of risk appetite is about helping organisations to articulate and control this.

#### Defining risk tolerance

The term risk tolerance may be used instead of risk appetite, especially where the focus is on downside risk. More accurately, the concept complements risk appetite and can be used to set tolerance limits for specific categories of risk, or for metrics such as risk, control or performance indicators.

Tolerance limits are best understood in the context of downside risks. An organisation may set tolerance limits for health and safety incidents. Minor incidents may be tolerated, but not major incidents such as a death or serious injury.

In terms of metrics, tolerance limits may be set for a range of risk, control or performance indicators including staff turnover rates, staff absence rates, customer complaints, system availability, late audit items or cash-flow volatility.

Tolerance limits can be linked to the concept of RAG reporting. Any risk or metric that is in the red zone will generally be considered intolerable, with the boundary between amber and red denoting the limit of tolerance. The boundary between green and amber may be used to show the preferred limit of tolerance.

#### Defining risk capacity

Risk capacity denotes the maximum enterprise-wide level of risk to which an organisation may be exposed.

Decisions that increase an organisation's exposure to risk can add up. An organisation may get into trouble if several of these result in unfavourable outcomes at the same time. An organisation may need to take risks to achieve its objectives but if it takes too much risk in aggregate it will risk serious financial distress and ultimately bankruptcy.

Risk capacity is usually a function of an organisation's financial strength. Organisations that have significant financial reserves or low levels of debt can normally take more risk.

Risk capacity may also be determined by governments, regulators or other stakeholders (such as shareholders and consumers). For example, public concern about the risks associated with activities such as fracking or genetically modified foodstuffs may mean that organisations decide against investing in them despite the potential financial returns. Equally, banks may wish to lend more money to generate greater profits, but regulators may prevent them from doing so because of concerns about the risk to the financial system.

*Different organisations used different terminology for risk appetite, tolerance and capacity, and often use the terms interchangeably. This can cause confusion for organisations, so it is important to decide on and then consistently use the terms.*

#### **Risk appetite as a mechanism for balancing risk and return**

Exposure to risk can create the potential for positive as well as negative outcomes. Strategic level risks – such as developing a new product or service, increasing output,

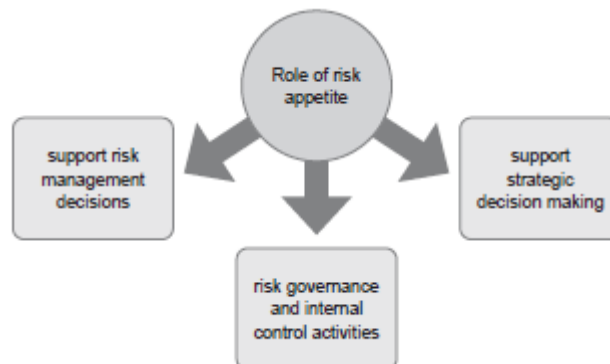
implementing a new IT system or merging with another organisation – come with the potential for profit and loss. Financial risks, such as market and credit risk, also have the potential for upsides and downsides.

Even where risks only have a downside, as in the case of health-and-safety compliance or environmental risks, it is rarely possible to eliminate these risks completely. This may be because the cost would be too high or because, whatever the expenditure on control, a degree of residual risk will remain as long as a particular activity or process remains in operation.

Because exposure to risk may have positive and negative outcomes and because it is rarely practical to eliminate risk, an organisation should decide what risks to take and the level of risk exposure that is optimal. By determining and communicating its appetite for risk, an organisation can ensure that risk and return is balanced in a logical and consistent way and ensure that downside risks are controlled in a cost-effective way.

### **How risk appetite can support decision making and the maintenance of appropriate corporate governance**

There are three roles that risk appetite plays as shown in the figure below:



#### Risk-management decisions

A common role for risk appetite is to act as a benchmark for risk-management decisions. This helps to determine whether a given level of risk is 'within appetite'.

Risk appetite can be used to identify:

- the risk events that an organisation should reduce its exposure to, because the exposure to downside losses is too high;
- the risk events that need relatively little attention because exposure is 'on appetite'; and
- the risk events that an organisation should increase its exposure to, because opportunities may otherwise be missed.

By determining its appetite, an organisation can allocate its limited risk-management resources more efficiently – targeting resources where they are needed the most – to reduce the exposure to risks that are above appetite, or to increase exposure where the level of risk is too low. In addition, determining risk appetite should help to improve buy-in for risk-management activities by highlighting the negative consequences of not maintaining appropriate levels of risk exposure.

Managers and employees can perceive risk management as a tool that leads to excessive control and conservatism. The concept of risk appetite provides a clear benchmark for risk-reducing and risk-increasing activities, preventing over control and excessive risk-taking.

### Risk governance and internal control

The concept of risk appetite has an important role to play in maintaining appropriate corporate governance. By expressing, setting and monitoring its appetite for risk an organisation can constrain management decision-making, ensuring that they do not expose it to an excessive amount of risk or make overly conservative decisions that generate an insufficient return. This should help an organisation to achieve its objectives and satisfy the needs of stakeholders.

Within a governance and internal control context, it is common to use risk appetite as a mechanism for limit setting, where limits are set for an organisation's total exposure to risk or for specific categories and types of risk event.

Care should be taken when using the concept of risk appetite to set absolute limits for risk exposure. Logically it does not make sense to set absolute limits for risk exposure, since increased levels of risk may be associated with higher levels of return. It is more logical to set relative limits in terms of the rate of return that may be required for a specific level of risk.

This is sometimes known as the risk premium. This risk premium helps to further clarify the balance that an organisation needs to maintain between risk-taking and generating a return or delivering a service.

In finance and accounting terms, the concept of risk-adjusted return is one way in which a risk premium can be expressed. A return that is risk adjusted is discounted to reflect the potential for downside losses. The greater the exposure to downside loss, the greater the discount rate. The returns on risky financial market investments are often risk adjusted to reflect the level of risk exposure.

### Strategic decision-making

Determining an organisation's appetite for risk supports strategic decision-making and the achievement of its objectives.

An organisation without a clear appetite for risk might pass up value-adding opportunities because they do not have a clear understanding of how to balance risk and return. In contrast, another organisation might make strategic decisions that expose it to high levels of risk in order to generate positive returns, but the level of return that is generated may be relatively low.

An organisation cannot make effective strategic decisions if it does not have a consistent benchmark to help it weigh up the positive and negative outcomes that might occur as a result of these decisions. It is not sufficient to assess returns and risk exposure: an organisation must decide whether the level of return is sufficient for the risk taken. Without an understanding of its appetite for risk, an organisation may make inconsistent decisions that expose it to too much or too little risk.

By helping to articulate the degree of risk that it is willing to take for the returns that may be generated, risk appetite can be used to ensure that an organisation:

- does not enter into investments or activities that expose it to an excessive amount of risk, where the potential for return is too low to compensate for the potential for downside losses; and
- is not overly conservative: stifling innovation, promoting excessive bureaucracy, and passing up investments or activities that should add value.

*As noted in the case study and question, RichGold has overlooked opportunities in the past, which may be due to the lack of understanding and consistent use of risk appetite*

*within the company. It appears that not everyone was aware of how risk is too much risk, although the previous CEO of Gold had a low risk appetite, which may not be reflected by the new Board.*

### **Determining risk appetite**

Care is needed when determining an organisation's appetite for risk. If risk appetite is set too low then valuable opportunities may be missed. If risk appetite is set too high, then an organisation may become financially distressed and have to cease operating.

#### Factors to consider when determining appetite

Various factors may influence the level of risk appetite chosen by an organisation. Common factors include:

- legal and regulatory requirements;
- the risk preferences of key stakeholder groups such as shareholders, customers and employees;
- the specialist knowledge, skills and experience of the organisation's risk, compliance and governance specialists (highly skilled specialists may be able to help an organisation take risks that have a greater upside potential);
- the strength of an organisation's balance sheet, which will influence its ability to withstand unexpected losses – high levels of capital resources are especially significant, as is the ratio of debt to equity; and
- external factors such as technological change or economic growth.

Technological change, such as the emergence and expansion of the internet and social media, can present significant upside opportunities and downside threats. Examples of high-risk-appetite companies looking to exploit technological change include Tesla and Uber.

Organisations may decide to increase their appetite for risk in the face of technological change, risking large losses in the hope of exploiting opportunities that may generate big financial gains. Periods of high economic growth may also promote risk-taking because of the increased opportunity for profit. Investment risk appetite levels tend to increase during periods of economic growth. Should this growth stop, then an organisation may experience larger than expected losses.

Great care is needed when deciding whether to exploit a period of economic growth, as illustrated by the losses some banks suffered during the 2007–08 financial crisis.

*The complex nature of the mining industry and the preferences of stakeholders will have an effect on the determination of RichGold's risk appetite. Since the departure of the previous CEO of Gold, the merger of the two companies and the Board's remit to look for opportunities, the risk appetite will be different. In addition, the lower profits may influence the risk appetite, although it may not be considered a major issue as this was mainly due to the one off costs of the merger.*

### **The role of the board in determining risk appetite**

An organisation's risk appetite should usually be set by the board or trustees. This expectation is reflected in many governance codes, including the UK Governance Code. In some organisations, risk appetite is decided below board level and sent to them for approval. This is not good practice. The board should play an active role in determining an organisation's appetite for risk. When setting an organisation's appetite for risk, the board should consider the factors highlighted in the previous section.

	<p>The board is best placed to determine risk appetite because it has a broad organisation-wide view and exists to represent the interests of stakeholders. The board is also often responsible for determining strategy and an organisation's objectives. These are factors that influence and are influenced by risk appetite.</p> <p><i>Clearly the Board have the responsibility to determine RichGold's risk appetite.</i></p> <p><u>The role of the chief risk officer and risk function</u></p> <p>Where an organisation has a CRO or risk function, they should help to facilitate the board's role in setting risk appetite. This might include organising a workshop or providing information to help the board make a decision.</p> <p>The CRO or risk function plays a key role in helping an organisation to monitor its risk profile relative to its risk appetite. This can be achieved through the production of risk reports. The CRO or risk function can provide expert risk control advice where an organisation is taking too much or too little risk relative to its risk appetite.</p>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Level	Mark	Descriptor
	0	No rewardable material.
<b>Level 1 (Fail)</b>	1-12	<ul style="list-style-type: none"> <li>• The answer gives an incomplete or incorrect understanding of the risk appetite.</li> <li>• The answer provides an incomplete or incorrect definition of risk appetite, risk tolerance and risk capacity.</li> <li>• The answer provides incomplete or incorrect understanding of the role of risk appetite in supporting decision making and maintaining corporate governance.</li> <li>• The answer gives an incomplete or incorrect understanding of how the Board might determine their risk appetite.</li> <li>• The answer provides an incomplete or incorrect information on the Board's role in determining an organisation's risk appetite.</li> <li>• The answer makes few, if any, links between the theory and practice, using the case study.</li> </ul>
<b>Level 2 (Pass)</b>	13-16	<ul style="list-style-type: none"> <li>• The answer provides a basic understanding of risk appetite.</li> <li>• The answer provides a basic definition of risk appetite, risk tolerance and risk capacity.</li> <li>• The answer provides a basic understanding of the role of risk appetite in supporting decision making and maintaining corporate governance.</li> <li>• The answer provides an overview of how the Board might determine their risk appetite.</li> <li>• The answer provides an overview of the Board's role in determining an organisation's risk appetite.</li> <li>• The answer includes clear links between theory and practice, using the case study.</li> </ul>
<b>Level 3 (Merit / Distinction)</b>	17-25	<ul style="list-style-type: none"> <li>• The answer illustrates a clear and strong understanding of risk appetite.</li> <li>• The answer gives a strong and comprehensive definition of risk appetite, risk tolerance and risk capacity.</li> </ul>

		<ul style="list-style-type: none"><li>• The answer provides a clear and comprehensive understanding of the role of risk appetite in supporting decision making and maintaining corporate governance.</li><li>• The answer illustrates a clear and comprehensive understanding of how the Board might determine their risk appetite.</li><li>• The answer gives a strong and comprehensive understanding of the Board's role in determining an organisation's risk appetite.</li><li>• The answer makes strong links between theory and the case study, which is supported with appropriate examples both from the case study and the real world.</li></ul>
--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

PILOT PAPER

4. There have been large scale changes in the mining industry, from increases in the use of automation and innovative technologies through to the need to stay in step with the rapidly changing demands and expectations of society.

These structural changes have had an impact on RichGold which has not yet been fully recognised or understood in relation to its human capital. Suchitra is also concerned about the impact of the merger and the change management initiatives that are being undertaken.

Due to the problems with the board members originally from Rich and Gold, Suchitra has asked you to introduce the subject at the next Board meeting.

Prepare a paper for the Board, evaluating the risks around human capital and changing knowledge and skills that are relevant to RichGold. The paper should include:

- at least **three** further examples of structural changes in the workplace affecting human capital
- at least **three** examples of the problems in sourcing talent
- the training and management of talent from the perspective of controls for managing human capital risks,
- the Board's role in managing talent risks to ensure they have the right workforce for the future.

(25 marks)

Question number	Indicative content
4 25 marks	<p>Answers should provide confidence to the markers that the candidate has understood and demonstrated their learning in relation to risks to human capital and changing knowledge and skills. It is expected that candidates provide at least <b>three</b> examples of structural changes in the workplace affecting human capital and <b>three</b> examples of problems in sourcing talent.</p> <p>In addition, candidates are expected to demonstrate that they understand talent training and talent management as controls for managing human capital risks. Candidates are also expected to demonstrate that they understand the role of the Board in managing talent risks to ensure they have the right workforce for the future. It is not expected that candidates include information on talent risk management frameworks, but where this is included in the answer, an additional two marks, in total, can be awarded by the markers. The answer should be formatted as a paper for the Board and include clear links to the case study.</p> <p><b>Answers could include the following content:</b></p> <p><b>Structural changes in the workforce</b></p> <p>Human capital is one of the most important intangible assets an organisation has. These are the people who will be making decisions and driving business strategy in an increasingly turbulent business environment.</p> <p>Attracting the right talent (skilled, educated and adaptable employees) should be a key priority of the senior management team and the board. In fact, talent management is a business strategy in itself. Over the last decade, there have been a number of structural changes in the workspace in general:</p> <ul style="list-style-type: none"> <li>• With increased globalisation and advances in technology, more and more low to mid-level jobs are being outsourced to emerging markets or computers. For example, a number of studies suggest that London will lose one-third of such jobs in the next 20 years, specifically highlighting jobs such as retail, storage and</li> </ul>

transportation being at the highest risk of automation. Specialist jobs such as doctors and teachers are seen to be less at risk, although certain level of disruption is expected.

- Rapid advances in technology require continuous employee training in order that organisations remain agile and up to- date with the latest business intelligence tools.
- Millennials – who now account for the largest segment in the workforce – demand a purposeful and personalised type of employment.
- Reporting structures within organisations have become flatter in order to encourage innovation.
- The drive for diversity has created more inclusive working environments.
- With a significant increase in the use of flexible working arrangements and higher mobility of people in general, organisations have to rethink how they remotely manage and train their employees.

In addition, the gap between skills possessed by employees and the skills required by organisations is becoming wider. Employees' skills and experience are becoming less valuable faster than in the past, due to the speed of change in internal and external environmental business factors.

*Candidates can include the examples given in the question, but it is expected that three further examples of structural changes are provided. Increased globalisation and use of technology would be examples relevant to RichGold, especially as they are actively pursuing this in their strategy. In addition, Millennials, the drive for diversity and flexible working environments would have a large impact on a company in the mining sector.*

#### In-demand skills

With rapid advances in technology and a shift towards digital culture, skills like data science, application development, cloud computing, digital marketing and advanced statistical modelling are in demand.

In addition, many roles increasingly combine a need for in-depth specialist knowledge and an aptitude for 'big picture thinking'. Personality traits, such as attitude, motivation, curiosity, collaboration, adaptability and agility, are much sought after by prospective employers.

#### **Sourcing talent**

The traditional recruitment model involved organisations seeking applicants for base-level entry roles and then gradually promoting them internally. Having 'a job for life' was common. However, as people have become more mobile, employee turnover rates have increased dramatically – even in organisations that offer best-in-class training and development opportunities. This has forced organisations to tap into the market of external candidates across different managerial levels.

The traditional approach of simply advertising a vacant role on its own or through a specialist firm no longer guarantees that this position will be filled in a timely manner. Organisations have realised that hiring talent requires a well-thought-out process and creative sourcing tactics, such as:

- making use of social media platforms such as LinkedIn;
- forming partnerships with college communities;
- organising company insight sessions;
- creating talent referral programmes;
- building databases of prospective employees before vacancies are available;

- redesigning job specifications to explain how a particular job opportunity can benefit the applicant, instead of focusing on the needs of the employer. As a result, job ads are becoming more personalised and lighter on corporate jargon.

*Examples of problems sourcing talent could include the mobility of the workforce, the consideration that mining is often seen as a labour-intensive and unsafe occupation. In addition, the mining industry's traditional environmental and social reputation may not be appealing to prospective talent.*

### **Training talent**

Due to the increasing rate at which skills and knowledge become outdated, it is essential that organisations understand the importance of continuous training and development programmes in the workplace. Although expensive, training offers an opportunity to expand the knowledge base of all employees for the benefit of improved performance, job satisfaction and morale.

Employees who receive formal training are more confident, engaged and better able to perform their roles. Better performance increases productivity and reduces employee turnover, which benefits the overall organisation. It enhances the organisation's reputation and profile, which in turn makes it easier for this organisation to attract top talent.

Corporate mentoring schemes are an increasingly popular way to engage and train employees. It gives more-senior employees an opportunity to give back to the organisation and be directly involved in developing talent, while mentees benefit from valuable advice and access to important networks.

Some organisations also promote reverse mentoring initiatives, in which senior executives are mentored by younger employees on topics such as new technology and media trends. Jack Welch, former CEO of General Electric, has been widely credited with helping to promote reverse mentoring, when he committed himself and other senior executives to reverse training sessions dedicated to the internet in the 1990s.

Over the past few years, blended learning – a combination of classroom learning and online training has become a popular and more affordable option for developing employees.

### **Managing talent**

The 'war for talent', a term coined by McKinsey consultants in the late 1990s, is not a new concept. It refers to the highly competitive landscape for attracting and retaining talented employees. Talent has become a form of currency: an intangible asset that directly contributes to an organisation's profits and losses. Talent-management conversations now take place at board level. Even so, the skills gap has never been wider, despite organisations spending significant resources to find new talent.

To understand the impact of talent shortages, Manpower Group conducted a survey of 39,195 employers in 43 countries in 2018. The results were quite shocking: 67% of employers (with more than 250 employees) said they cannot find the skills they need. This feedback was consistent across different industries.

This survey also highlighted the fact that talent shortages have been growing over the past few years and are now at a 12-year high, with larger organisations facing greater challenges. The survey listed multiple reasons for why organisations are not able to fill open roles, with 27% of employers saying that applicants lack either professional skills or personal characteristics.

One of the drivers of the skills gap is the need for organisations to redefine jobs more frequently, as business requirements change to reflect a new environment. Likewise, organisational talent planning and talent management strategies need to change to remain relevant.

Organisations have realised that short-term 'plug-in' or 'one-size-fits-all' talent solutions are not very effective, as they ignore the need to structurally reconfigure talent needs in a sustainable way. Talent management has therefore become a strategic tool within human resource planning, aimed at creating value by means of aligning the organisation's business strategy with its workforce.

At its core, talent management as a business discipline sees employees as the only assets that innovate in an organisation, and innovation as the only path to sustain long-term performance. Proactively managing talent should create a competitive advantage for the organisation. Furthermore, talent management practices themselves are also meant to be continuously reviewed so that the organisation is able to capitalise on its talented employees in order to grow and expand into new markets.

The key components of talent management are:

- strategic employee planning that clearly connects the organisational strategy to talent needs;
- talent acquisition and retention that recognises the importance of in-house development;
- performance management that aligns the right person with the right role and aligns roles with the strategy;
- learning and career development programmes that are aligned with the organisational culture and strategy;
- compensation structures that recognise and reward employees based on their contributions towards maximising the long-term value of the organisation;
- succession planning that ensures the sustainability of the strategy execution process.

Talent management programmes are typically developed and managed by human resources. However, many organisations now employ a designated talent management executive tasked with developing strategies to attract, empower and retain talent. This executive typically has a direct communication line to the board.

### **Talent risk-management frameworks**

Talent risk is a business risk. Talent risk-management is the process of assessing the organisation's employee needs and its hiring capacity, compared to what skills are available internally and externally.

This process typically begins with an assessment of the business need for specific skills given the organisation's strategy. This can be due to an urgent need or as part of a long-term planning process. Residual talent risk should then be prioritised, mitigated, measured and monitored.

The central elements of talent risk assessment focus on organisational and employees' alignment, capability, cost, capacity, connection and compliance. Issues include:

- Potential misalignments between the current business strategy and the available internal talent pool.
- The ability to develop talent internally in order to meet future needs, including the breadth and depth of skills, qualities and unrealised potential of current employees.

- The cost of developing the existing workforce versus hiring external talent, including whether overall cost of the existing workforce is appropriate given the organisation's long-term strategy goals.
- The identification of critical roles, the retention of critical employees and the risks surrounding the succession into these roles. This includes considerations such as the ability to obtain required regulatory approvals. For example, organisations regulated by the FCA have to comply with the 'Approved Persons' regulation. This requires all employees who perform a governing function to seek a regulatory approval to become an 'approved person'.
- The risk of an organisation's top talent becoming disengaged, possibly due to a lack of cross-functional training opportunities, weak emotional connection with the company's leadership or lack of belief in the organisational mission.
- The risk of employees participating in talent programmes not complying with relevant laws and regulations.

For example, a US company may be looking to expand to the UK market in the next two to three years. This means the company must undertake a risk assessment of its talent to understand who it can source internally and who it will have to hire externally. Given that the project is two to three years away, the company may decide to launch a specialised training programme or prioritise certain training programmes over another to create a bigger pool of internal candidates.

This reduces the cost of looking for senior executives externally. The company can also conduct an external market scan to evaluate the cost of 'plugging the gap' between internal candidates and the number of employees required to successfully execute the expansion.

*It is clear that talent training and management is an important consideration for RichGold, especially during the current uncertainty and pressure on the human capital from the merger and the new initiatives. It will also influence the issues currently faced where training has not been consistent or embedded and where staff surveys have not been conducted since the merger.*

*If both training and management are implemented effectively, it will reduce the turbulence in staff turnover, and support recruitment and retention of key talent in the organisation.*

### **The role of the board**

The board plays a key role in overseeing the implementation of appropriate talent strategies and managing talent risks in line with the overall business objectives.

This role should not be underestimated. A 2016 KPMG survey identified senior leaders' lack of interest in connecting and engaging with their employees, poorly designed performance management processes, an insufficient budget for managing and developing talent, and a weak future leadership pipeline as key contributors to talent gaps.

The board should ensure that the organisation has an effective and robust talent management process in place which is capable of delivering value for stakeholders. Talent management oversight should not be delegated to management. To more effectively oversee talent risks, the board should ensure that:

- the organisation has an effective talent risk assessment and management framework in place. This framework should cover business, reputational, regulatory and compliance risks that are related to talent;
- the organisation has incorporated contingency planning and crisis management scenarios within its talent management framework, such as the sudden departure or illness or death of critical employees, poaching of entire critical teams by competitors and so on;

	<ul style="list-style-type: none"> <li>• Board members should have a direct oversight of how the CEO's and executive members' compensation packages are structured relative to overall strategy and performance;</li> <li>• senior leadership should be directly accountable for the execution of talent strategies;</li> <li>• issues such as diversity (gender, ethnicity, nationality and age) and pay gaps should be incorporated within the talent management framework;</li> <li>• the organisation should maintain a strong leadership pipeline with a succession planning process in place;</li> <li>• board members should have regular access to talent-related KPIs and risk discussions;</li> <li>• The board should appoint a designated talent management director or executive to address talent-related issues and risks.</li> </ul> <p>It is essential that the board understands and receives assurance from management that the talent risk is being proactively assessed, monitored and managed. These risks will only become more important as the business world becomes more complex and interconnected.</p> <p><i>It appears that the Board don't recognise any problems with the company's human capital, or has not previously been made aware of the issues. The paper should make it clear that Suchitra has an important role in improving that awareness and understanding.</i></p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Level	Mark	Descriptor
	0	No rewardable material.
<b>Level 1 (Fail)</b>	1-12	<ul style="list-style-type: none"> <li>• The answer is not formatted as a paper for the Board.</li> <li>• The answer gives an incomplete or incorrect understanding of the risks to human capital and changing knowledge and skills.</li> <li>• The answer provides an incomplete or incorrect understanding of structural changes in the workplace affecting human capital, with fewer than three examples that are relevant to the case study.</li> <li>• The answer provides an incomplete or incorrect understanding of the problems in sourcing talent, with fewer than three examples that are relevant to the case study.</li> <li>• The answer provides incomplete or incorrect understanding of talent training and talent management as controls for managing human capital risks.</li> <li>• The answer gives an incomplete or incorrect understanding of the Board's role in managing talent risks to ensure they have the right workforce for the future.</li> <li>• The answer makes few, if any, links between the theory and practice, using the case study.</li> </ul>
<b>Level 2 (Pass)</b>	13-16	<ul style="list-style-type: none"> <li>• The answer makes some attempt to be formatted as a paper for the Board.</li> <li>• The answer provides a basic understanding of the risks to human capital and changing knowledge and skills.</li> <li>• The answer provides basic information on the structural changes in the workplace affecting human capital, with at least three examples that are relevant to the case study.</li> <li>• The answer provides basic information on the problems in sourcing talent, with at least three examples that are relevant to the case study.</li> </ul>

		<ul style="list-style-type: none"> <li>• The answer provides a basic understanding of talent training and talent management as controls for managing human capital risks.</li> <li>• The answer provides an overview of the Board's role in managing talent risks to ensure they have the right workforce for the future.</li> <li>• The answer includes clear links between theory and practice, using the case study.</li> </ul>
<b>Level 3 (Merit / Distinction)</b>	17-25	<ul style="list-style-type: none"> <li>• The answer is well formatted as a paper for the Board.</li> <li>• The answer illustrates a clear and strong understanding of the risks to human capital and changing knowledge and skills.</li> <li>• The answer gives a strong and comprehensive understanding of the structural changes in the workplace affecting human capital, with more than three examples that are relevant to the case study.</li> <li>• The answer provides a strong and comprehensive understanding of the problems in sourcing talent, with more than three examples that are relevant to the case study.</li> <li>• The answer illustrates a clear and comprehensive understanding of talent training and talent management as controls for managing human capital risks.</li> <li>• The answer gives a strong and comprehensive understanding of the Board's role in managing talent risks to ensure they have the right workforce for the future.</li> <li>• The answer makes strong links between theory and the case study, which is supported with appropriate examples both from the case study and the real world.</li> </ul>

---

**TOTAL FOR SECTION A = 75 MARKS**

# Section B

Questions 5 and 6 do not relate to the pre-released case study. Answer one question.

5. As the Company Secretary of a large retail organisation you decided to progress your professional development and gain accreditation with the Chartered Governance Institute (CGIUKI). You successfully achieved Associate membership in 2019, and to maintain your professional status you became a visiting lecturer at a local university to share your knowledge with students through the University’s Business School.

With your background in retail, you have been asked to provide lectures to students from the retail sector who are part of the Degree Apprenticeship Scheme. As such, you will be educating mature students, some of whom have been in the industry for a number of years.

In your own role, you have witnessed a lack of formal knowledge of risk management by managers who come into your organisation, sometimes at senior levels. You have therefore asked if you can share your academic knowledge and practical experience in both risk identification and risk control, two areas that you believe have been insufficiently understood in your industry.

(a) To support your upcoming lecture on risk identification, write a paper assessing risk identification. Include in the assessment the purpose of risk identification and provide at least **three** non-analytical risk identification techniques, providing at least **one** example risk to the retail industry that might be identified using each of those techniques.

(15 marks)

Question number	Indicative content
5 (a) 15 marks	<p>Answers should provide confidence to the markers that the candidate has understood and demonstrated their learning in relation to risk identification. It is expected that candidates demonstrate that they understand the purpose of risk identification and provide at least <b>three</b> non-analytical risk identification techniques.</p> <p>Candidates are also expected to provide at least <b>one</b> example risk to the retail industry that might be identified using each of those three techniques.</p> <p>Candidates may include different examples of risks from their chosen risk identification techniques than the example in the marking scheme, it is only expected that the examples given are relevant to the identification technique and the retail industry.</p> <p>It is not expected that students provide information on analytical risk identification techniques, as the question explicitly requests information on non-analytical techniques. Where information is provided on analytical techniques in addition to the three non-analytical techniques, an additional two marks overall can be awarded. However, where analytical techniques are provided instead of non-analytical techniques, markers should consider this part of the question to be part-answered. Analytical techniques from the study text include: Structured what-if technique (SWIFT); Delphi technique; Root-cause analysis, and ; System and process mapping. The answer should be formatted as a paper and include clear links to the scenario.</p> <p><b>Answers could include the following content:</b></p>

### **Purpose of identifying risks**

An organisation is exposed to a wide range of risks. The purpose of risk identification is to determine the nature of these risks and the specific types of risk event that may occur. Potential risk events might include:

- a fire
- workplace accident
- fraud
- a creditor defaulting on a loan or credit agreement
- economic recession
- cyber attack
- a sudden reduction in consumer demand.

Positive risk events may also occur – such as a sudden increase in consumer demand – but upside opportunities are rarely the focus of formal risk-event identification activities, outside of narrow applications to risks like energy price fluctuations. This focus on the identification of downside risk (threats) is not necessarily desirable. Organisations should be identifying positive and negative risk events to support strategic decision-making. The risk identification techniques discussed here may be used to identify positive as well as negative risk events if desired.

A variety of different techniques can be employed to help identify risk events. These techniques vary in their sophistication. More sophisticated techniques are not necessarily better and can be costly to implement. An organisation's choice of techniques will depend on the nature, scale and complexity of its activities, as well as regulatory requirements.

### **Non-analytical techniques for identifying risks**

#### Expert judgement

Expert judgement relies on the skills and experiences of relevant specialists, either in isolation or working as a group.

For example, an IT specialist should have a good understanding of the types of IT-related risk events to which an organisation may be exposed. Equally, finance specialists should have a good understanding of any financial risks, such as the risk of making a financial misstatement.

Most organisations will use their own internal specialists to provide expert judgement, but in some circumstances external experts, such as risk-management consultants, may be used.

It is helpful to have a facilitator to work with experts to help them identify all relevant risks. The facilitator may be an internal risk specialist or an external consultant.

*An example of a risk identified using expert judgement might be the lack of sufficient IT security for an online retailer.*

#### Focus groups and surveys

Focus groups may comprise a mix of specialists, such as IT, finance and HR specialists. They may also include functional and departmental managers, such as operations managers or marketing managers.

The idea behind a focus group is to share a range of different perspectives and experiences to achieve a consensus view. This should ensure that a greater number of relevant risk events are identified. The cost is that focus groups take up more specialist or management time due to the greater number of people involved.

An alternative way to collect a range of views is via a risk survey. Here, relevant specialists and managers are asked a series of questions and their responses are consolidated and analysed to identify relevant risk events.

A simple risk identification survey may ask respondents to list the risk events that they believe could occur or may provide a checklist of potential risk events. More sophisticated surveys may ask about how organisational processes and procedures are designed and controlled to identify the potential sources of risk events. Risk events are often linked to weaknesses in process design or control failures. Surveys may be created by internal or external risk management specialists.

*An example of a risk identified using focus groups and surveys might be the weaknesses identified in the transfer and storage of stock, which has led to increased loss of products.*

### Checklists

Checklists provide a prepared list of potential risk events. Checklists are used to support other risk-identification approaches such as expert judgement, focus groups and surveys.

A checklist ensures that particular types of risk event are not forgotten. Experts, focus groups or survey respondents may accidentally overlook certain types of risk event. A checklist ensures that all relevant sources of risk are given consideration.

An organisation may draw up its own checklists based on their past experience of risk events, or use checklists provided by an external agency, such as risk-management association, consultant or regulator. The advantage of external agencies is that they are able to learn from the experiences of multiple organisations.

One example of an external checklist is the Basel loss event types (Basel Committee, 2009: Annex 7) that are used by most banks, other financial and non-financial institutions to help them identify operational risks, shown in the table below.

Level 1	Level 2
Internal fraud	Unauthorised activity (such as breach of policies and procedures) Theft and fraud
External fraud	Theft and fraud Systems security (cyber-attacks)
Employment practices and workplace safety	Employee relations (strikes and so on) Safe environment (health and safety) Diversity and discrimination
Clients, products and business practices	Suitability, disclosure and fiduciary (breach of privacy, aggressive selling and so on) Improper business or market practices (insider trading or money laundering) Product flaws (faulty products) Selection, sponsorship and exposure (exceeding client risk limits) Advisory activities (providing poor advice)
Damage to physical assets	Disasters and other events (natural disasters, terrorism and so on)
Business disruption and systems failure	Systems (hardware, software, telecoms, internet failure)

Execution delivery and process management	<p>Transaction capture, execution or maintenance (data-entry error, accounting error and so on)</p> <p>Monitoring and reporting (financial reporting misstatement or reporting error to regulator)</p> <p>Customer intake and documentation (errors in product documentation or marketing campaign and so on)</p> <p>Customer/client account management (negligent loss of client funds or some other management error)</p> <p>Trade counterparties (poor performance or disputes)</p> <p>Vendors or suppliers (poor performance or disputes)</p>
-------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

One feature of the Basel event types is that they are presented in different levels. Level 1 and Level 2 are shown in the Table.

This approach allows an organisation to choose a more or less detailed checklist, assisting with the categorisation of identified risks. It is clear from the table how a specific Level 2 risk event relates to the Level 1 risk events.

More detailed checklists facilitate more targeted risk assessment monitoring and control activities. They also reduce the chance that important risk events may be overlooked but they increase the amount of time that must be devoted to risk identification. An organisation must balance the costs and benefits of more or less detailed checklists and choose the approach that works best for its circumstances.

*An example of a risk identified using checklists might include any of the examples shown in the table above. Even though they relate to the financial services sector many of these are also relevant to the retail sector.*

The benefits and costs of checklists can be seen in the Table below.

Benefits of checklists	Costs of checklists
A cheap and efficient way of collating large amounts of information.	Can be used by someone who may not be skilled in the subject of the checklist.
Simple and easy to use. Ensures that relevant sources of risk are not missed	Can be completed by someone who may not understand precisely the objectives and ultimate use of their answers.
A useful way of updating information for current use and for monitoring trends against previous surveys.	Can focus the user's attention simply on completing the checklist, without keeping the overall reason for the checklist in mind, causing the task to be seen as just a 'form filling' exercise.
Can be adapted to individual areas of risk focus (such as health and safety, environment and so on).	May be ambiguous to the reader, however careful the design.
Useful for putting diverse sources of information into a common format.	May be completed too quickly, and therefore without much thought, by someone who considers that their own time is better spent elsewhere.
Can be used to provide evidence of compliance with relevant risk-management regulations.	May be completed by someone who has their own reasons for suppressing risk information.

	<p><u>Physical inspections</u></p> <p>Physical inspections of workplaces are a common way to assess health-and-safety-related risks or risks relating to fire and other physical hazards.</p> <p>Physical inspections are usually completed by qualified risk-identification specialists such as a building surveyor, fire-safety professional or health and safety expert. Inspections are often supported by the use of questionnaires or checklists to ensure that nothing important is missed.</p> <p>There is a clear advantage when a workplace and its employees are visited, particularly by someone who has the specialised knowledge to take a professional view of what is there. A formal inspection report will normally conclude with recommendations to improve the control environment and reduce the probability and impact of loss.</p> <p>The disadvantages of inspections are:</p> <ul style="list-style-type: none"> <li>• An inspector can only see risk exposures that are visible on the day of the visit. A visit is a snapshot in time and can capture only the activity of the day.</li> <li>• An inspection programme can be expensive, especially when visits are needed across many different workplaces.</li> <li>• Some of an organisation's greatest types or sources of risk may be those where third-party suppliers provide goods and services. The organisation may have difficulty obtaining authority to conduct detailed inspections in third-party premises unless this permission is negotiated within the original contract.</li> <li>• Risk-management is and should remain the responsibility of every manager and employee throughout an organisation. Regular visits by an inspector, if not carefully managed, could encourage managers and employees to believe that they can abdicate responsibility for risk-management to the inspector.</li> </ul> <p><i>An example of a risk identified through physical inspections might be the storage of more chemicals allowed or storage of incompatible materials for cleaning purposes which could lead to damage to the premises and the environment or harm to individuals.</i></p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Level	Mark	Descriptor
	0	No rewardable material.
<b>Level 1 (Fail)</b>	1-7	<ul style="list-style-type: none"> <li>• The answer is not formatted as a paper.</li> <li>• The answer gives an incomplete or incorrect understanding of the purpose of risk identification.</li> <li>• The answer gives an incomplete or incorrect information on less than <b>three</b> non-analytical risk identification techniques.</li> <li>• The answer gives incomplete or incorrect information as an example of risks raised using each of the chosen risk identification techniques.</li> <li>• The answer makes few, if any, links between the theory and practice, using the scenario.</li> </ul>
<b>Level 2 (Pass)</b>	8-9	<ul style="list-style-type: none"> <li>• The answer makes some attempt to be formatted as a paper.</li> <li>• The answer provides an understanding of the purpose of risk identification.</li> <li>• The answer provides basic information on at least <b>three</b> non-analytical risk identification techniques.</li> </ul>

		<ul style="list-style-type: none"> <li>• The answer provides a basic information on at least one example of a risk raised using each of the chosen risk identification techniques.</li> <li>• The answer includes clear links between theory and practice, using the scenario.</li> </ul>
<b>Level 3 (Merit / Distinction)</b>	10-15	<ul style="list-style-type: none"> <li>• The answer is well formatted as a paper.</li> <li>• The answer provides a strong and comprehensive understanding of the purpose of risk identification.</li> <li>• The answer illustrates a clear and strong understanding on at more than three non-analytical risk identification techniques.</li> <li>• The answer provides a comprehensive demonstration of more than one example of a risk raised using each of the chosen risk identification techniques.</li> <li>• The answer makes strong links between theory and the scenario, which is supported with appropriate examples both from the scenario and the real world</li> </ul>

PILOT PAPER

- (b) To support your lecture on risk control, write a paper assessing the reasons for risk control and the **five** common strategies for risk control (not risk treatment techniques), with **one** example of controls relevant to retail risks that might be considered for each of the five options. (10 marks)

Question number	Indicative content												
5 (b) 10 marks	<p>Answers should provide confidence to the markers that the candidate has understood and demonstrated their learning in relation to risk controls. It is expected that candidates assess the reasons for risk control and provide information on all <b>five</b> of the common strategies for risk control – the 5Ts.</p> <p>Candidates are also expected to provide at least <b>one</b> example control relevant to the retail industry that might be considered for each of the five options. Where information is provided on risk treatment techniques, including PCDD and common risk treatment controls, no marks will be awarded as they have been explicitly excluded in the question.</p> <p>The answer should include clear links to the case study.</p> <p><b>Answers could include the following content:</b></p> <p><b>Reasons for risk control</b></p> <p>All organisations make use of risk-control strategies and their associated control tools. These strategies and tools are used to reduce the probability and impact of loss events, such as fires, fraud or IT system failures.</p> <p>Risk-control strategies may also be used to increase the upside of risk events. From a risk-management perspective, risk control in organisations is focused on the prevention and reduction of loss event probabilities and impacts.</p> <p><u>Managing probability and impact</u></p> <p>An organisation may reduce its exposure to loss events by lowering the probability that a given event will occur or by mitigating the impact of any event that does occur. Risk-control tools that reduce the probability of a loss event occurring are known as loss-prevention tools. Tools that reduce the impact of loss events are known as loss-reduction tools. The following table provides examples of these tools.</p> <table border="1" data-bbox="316 1514 1465 1850"> <thead> <tr> <th data-bbox="316 1514 887 1565">Loss-prevention tools</th> <th data-bbox="887 1514 1465 1565">Loss-reduction tools</th> </tr> </thead> <tbody> <tr> <td data-bbox="316 1565 887 1624">IT system firewall</td> <td data-bbox="887 1565 1465 1624">Data backup arrangements</td> </tr> <tr> <td data-bbox="316 1624 887 1682">No-smoking policy</td> <td data-bbox="887 1624 1465 1682">Fire extinguishers</td> </tr> <tr> <td data-bbox="316 1682 887 1740">Segregation of duties</td> <td data-bbox="887 1682 1465 1740">Whistleblowing arrangements</td> </tr> <tr> <td data-bbox="316 1740 887 1798">Door locks</td> <td data-bbox="887 1740 1465 1798">Burglar alarm</td> </tr> <tr> <td data-bbox="316 1798 887 1850">Driver safety training</td> <td data-bbox="887 1798 1465 1850"></td> </tr> </tbody> </table> <p>To distinguish between loss-prevention and loss-reduction tools, consider the life cycle of a loss event.</p> <p>Loss-prevention tools reduce the probability of a loss event by targeting its causes. The causes of a loss event are usually linked to the actions or inactions of people, failures in processes and systems, or external events (weather, politics and so on). Loss events often require more than one cause to occur. For example, a fire may require faulty electrical wiring to cause a spark, plus combustible materials to burn.</p>	Loss-prevention tools	Loss-reduction tools	IT system firewall	Data backup arrangements	No-smoking policy	Fire extinguishers	Segregation of duties	Whistleblowing arrangements	Door locks	Burglar alarm	Driver safety training	
Loss-prevention tools	Loss-reduction tools												
IT system firewall	Data backup arrangements												
No-smoking policy	Fire extinguishers												
Segregation of duties	Whistleblowing arrangements												
Door locks	Burglar alarm												
Driver safety training													

Loss-reduction tools target the effects of loss events. Loss events may have financial and non-financial effects. In financial terms, they can affect the resources (physical assets and cash assets) of an organisation. Physical assets may be damaged or destroyed, requiring repair or replacement. Cash assets may be lost via fines or liability claims.

Loss-reduction tools reduce the financial effects of loss events by limiting the physical damage that is caused (such as by having a sprinkler system to put out a fire as quickly as possible), or by helping to fund the repair or replacement of loss assets, compensation payments or legal-liability claims as cost effectively as possible. Insurance is one way in which the repair or replacement of lost assets and compensation and liability claims can be funded.

In non-financial terms, loss events may cause death and injury. Loss events may also affect the reputation of an organisation via lost customer goodwill or adverse media coverage, for example. These can have an indirect financial value (such as loss of sales). The non-financial effects of loss events may be mitigated by shortening the duration of a loss event or by helping an organisation to recover quickly from events. Loss-reduction tools may also help to prevent death or injury, such as the use of evacuation arrangements in the event of a fire.

An organisation will employ a range of loss-prevention and loss-reduction tools to control particular loss events. In part, this is due to the fact that events are the result of multiple causes and have multiple effects. It is rare for any one risk control tool to combine probability and impact reduction.

#### Using controls for loss events to help seize opportunities

From a risk-management perspective, risk control is focused on preventing the causes and reducing the effects of loss events. From a wider strategic management perspective, risk control may help an organisation to seize opportunities for higher levels of financial and non-financial performance, allowing it to achieve and sometimes exceed its objectives.

Traditional loss-prevention and loss-reduction tools can help an organisation to seize opportunities by protecting its cash flows. An organisation needs cash to help it to exploit opportunities, such as exploiting new technologies, markets or opportunities to develop new products.

Mechanisms such as market research, and strategic investments such as flexible manufacturing systems or IT systems, can help organisations to seize new opportunities. As a risk-control tool, market research can be used to highlight and take advantage of potential opportunities for new product ideas and markets. Flexible manufacturing and IT systems allow organisations to adapt their production processes, modifying their products and services to exploit changes in customer needs and wants. For example, technological innovations that allow an organisation to supply products and services over the internet is a form of risk control, as it helps to protect an organisation's market share from competitors developing similar delivery mechanisms.

#### **Five common risk control strategies**

Controlling risk to manipulate the probability or impact of loss events, or to exploit opportunities, is not a given. Usually some kind of risk-control strategy is required. Five common options are:

- tolerate
- treat
- transfer

- terminate
- take the opportunity

### Tolerate

To tolerate a risk exposure means to take no formal action to control it.

Risks may be tolerated where they are known and accepted by an organisation. This may be where a risk exposure is considered to be within an organisation's appetite for risk.

In addition, an organisation may tolerate a risk where active controls are considered uneconomic or impractical, or where the risk is necessary to support the achievement of organisational objectives. Objectives such as the development of new products, process change or the implementation of new technology systems will always require a degree of risk.

The issue is that risk should be accepted on an informed basis.

Where risk exposures are tolerated, it is good practice for senior management to approve and periodically review the decision. It is rare for a risk exposure to be tolerated indefinitely.

*An example of a retail risk that might be tolerated is low level fraud or theft, where small value items are stolen either by customers or staff, but the actions needed to control the risk far outweigh the loss. However, the risk is monitored to ensure the number of small value thefts do not increase, at which point other risk control strategies would need to be considered.*

### Treat

Risk treatments are actions taken to manipulate an organisation's exposure to one or more risks, either to mitigate threats or to exploit opportunities. Risk treatments include many of the loss-prevention and loss-reduction tools that can be used by an organisation. It can also mean the increase of risk by increasing exposure or lowering controls.

*An example of a treatment control would be the introduction of loss prevention or loss reduction tools that would address the causes or effects of a risk, such as security tags and security barriers to reduce the risk of theft or the use of business continuity plans to reduce the impact of an unexpected store closure.*

### Transfer

Risk transfer passes the impact of loss events to a third party. This may involve passing on:

- the financial impacts of a loss event; or
- the financial and non-financial impacts of a loss event.

Passing on only the financial impacts of a loss event is achieved via insurance or equivalent risk-financing contracts.

Insurance contracts provide either full or partial indemnity against certain pre-specified loss events in return for the payment of a consideration or premium. The purchaser of an insurance contract, called the policyholder, is able to pass on the financial liability of one or more loss events to the insurance company, swapping volatility in their cash flows for a known cost in the form of an insurance premium. Other forms of risk financing work in a similar way.

Passing on the financial and non-financial impacts of a loss event involves a contract with a different type of third party, usually a supplier or outsourced service provider. Whenever

an organisation uses an external supplier to provide goods and services, it is effectively transferring the risks associated with the production and supply of these goods and services to the third party.

*An example of a transfer control would be the employment of a security company to provide the physical security at retail premises, or to provide the electronic surveillance in those premises.*

Terminate

Termination includes any action taken to stop an activity or leave a location that is creating a particular risk exposure or combination of exposures. For example, an organisation might decide to vacate premises with a high risk of flooding, or it might decide to stop using an operational process that creates a risk of environmental pollution or new technology that has a high risk of failure.

The decision to terminate a risk exposure is a very serious one. The only way to terminate an exposure is to terminate the activity or location that is creating the exposure. This could mean that an organisation passes up valuable opportunities and it may fail to achieve its objectives. The achievement of organisational objectives will always require activities that involve exposure to risk.

The decision to terminate a risk exposure should only occur where no level of risk exposure is considered to be tolerable, or where the risk exposure is considered to be untreatable or non-transferrable.

*An example of a terminate control would be the closure of retail stores in places where the security of staff is at risk, or the expectations of customers and stakeholders is that the organisation should not be operating in those areas, countries or regions.*

Take the opportunity

Remembering that risks represent both opportunities and threats, the final option involves taking the available opportunity or opportunities. When taking an opportunity an organisation may still implement other types of controls (e.g. risk treatments and transfers), either to mitigate any associated threats or to increase the potential to exploit the opportunity.

The option to 'take the opportunity' is present in activities such as corporate mergers, new product development and research and development. Such activities are risky and may involve both positive and negative outcomes. However, not taking an opportunity may sometimes be a bigger risk than taking one.

*An example of take control for the retail sector would be the entrance into a new market or the introduction of a new product line for an organisation before their competitors.*

Level	Mark	Descriptor
	0	No rewardable material.
<b>Level 1 (Fail)</b>	1-4	<ul style="list-style-type: none"> <li>• The answer is not formatted as a paper.</li> <li>• The answer gives an incomplete or incorrect understanding of the reason for risk controls.</li> <li>• The answer gives an incomplete or incorrect information on less than <b>five</b> common strategies for risk control.</li> </ul>

		<ul style="list-style-type: none"> <li>• The answer gives incomplete or incorrect information as an example of controls relevant to the retail industry that might be considered for each of the options.</li> <li>• The answer makes few, if any, links between the theory and practice, using the scenario.</li> </ul>
<b>Level 2 (Pass)</b>	5-6	<ul style="list-style-type: none"> <li>• The answer makes some attempt to be formatted as a paper.</li> <li>• The answer provides an understanding of the reason for risk controls.</li> <li>• The answer provides basic information on the <b>five</b> common strategies for risk control.</li> <li>• The answer provides a basic information on at least one example of a control relevant to the retail industry that might be considered for each of the five options.</li> <li>• The answer includes clear links between theory and practice, using the scenario.</li> </ul>
<b>Level 3 (Merit / Distinction)</b>	7-10	<ul style="list-style-type: none"> <li>• The answer is well formatted as a paper.</li> <li>• The answer provides a strong and comprehensive understanding of the reason for risk controls.</li> <li>• The answer illustrates a clear and strong understanding on the <b>five</b> common strategies for risk control.</li> <li>• The answer provides a comprehensive demonstration of more than example of a control relevant to the retail industry that might be considered for each of the five options.</li> <li>• The answer makes strong links between theory and the scenario, which is supported with appropriate examples both from the scenario and the real world</li> </ul>

6. Craster Electrical (Craster) is a large private sub-contractor in the construction industry, with 720 employees, an annual turnover of approximately £300m and a profit of £22 million. While the turnover has been consistent over the last three years, the profit levels have reduced from 11% to the current level of just over 7%.

In an effort to understand the reduction in profit level this year, the Board, through the Audit Committee, requested an external audit of their three key projects. Findings from the audit report showed that some key controls are not working effectively and that in a number of areas are showing non-compliance.

To support a business case being put forward by the CRO to introduce more consistent and value adding compliance management, assess compliance management frameworks for Craster.

Include the following points in the assessment:

- Why compliance management should be important to Craster, including the Board's responsibility and at least **six** examples of the consequences of non-compliance
- What **two** types of compliance standards organisations are usually tested against, with **one** example standard for each type of compliance standard relevant to a supplier or the construction industry, and
- The key components of developing a compliance management framework.

(25 marks)

Question number	Indicative content
<p>6 25 marks</p>	<p>Answers should provide confidence to the markers that the candidate has understood and demonstrated their learning in relation to compliance management frameworks. In addition, candidates should demonstrate that they understand why compliance management should be important, including the Board's responsibility towards the subject.</p> <p>Candidates should also demonstrate that they understand the <b>two</b> types of compliance standards that organisations need to observe and the four key components of developing a compliance management framework. Candidates are also expected to provide <b>one</b> example standard for each type of compliance standard relevant to a supplier or the construction industry. The answer should include clear links to the scenario.</p> <p><b>Answers could include the following content:</b></p> <p><b>Why compliance management should be important.</b></p> <p>Governance and compliance frameworks are a necessary component of effective risk-management. Without governance and compliance frameworks for risk-management, organisations will be vulnerable to bad behaviour on the part of their employees, including negligence or criminal activity. Numerous scandals, such as the VW emissions scandal, highlight the potentially severe consequences of bad behaviour.</p> <p>In addition, effective governance and compliance frameworks for risk management help all employees to understand the 'rules' regarding risk management, including the risks that can be taken to support the achievement of objectives and those risks that are out of bounds. However, while governance and compliance frameworks are necessary, they are not sufficient on their own. Equally important is culture and risk culture, particularly the tone from the top in relation to risk-taking and control.</p> <p>Compliance-management frameworks are necessary to ensure:</p>

- compliance with an organisation's internal policies and procedures;
- compliance with applicable laws and regulations (such as health-and-safety or environmental regulations)
- compliance with standards, guidelines and codes of conduct that the organisation has chosen to comply with, such as ISO 31000.

Problems arise when employees are not competent in their role or, for whatever reason, do not comply with the relevant policies, procedures and codes. This can lead to inappropriate risk-taking and significant control weaknesses. Cases such as the VW emissions scandal and the Barclays LIBOR scandal are examples of the serious consequences associated with weak controls and inappropriate risk-taking.

Cases like the VW or Barclays scandals are rare and extreme, but less severe risk-management-related governance and compliance issues are common. Examples include:

- not following health-and-safety procedures (neglecting to wear safety equipment or not performing a display screen risk assessment for an at risk employee);
- taking excessive amounts of financial risk, such as investing too much money in high-risk commodities or stocks and shares;
- non-compliance with expenses policies (claiming more than the allotted amount for meals or travel);
- fraud and the theft of company assets;
- diversity and discrimination issues;
- breaching financial mandates (such as budget approval limits or investment limits);
- not reporting serious risk events to senior management;
- hiding control weaknesses;
- sharing personal access passwords;
- taking data outside the organisation, including leaking sensitive data;
- not declaring any conflicts of interest; and
- accepting a bribe.

All these examples may have financial consequences for an organisation and could lead to regulatory enforcement action or adverse media reporting. They will also divert management attention from strategic and operational priorities. Effective governance and compliance should prevent these adverse outcomes and increase the chance that an organisation will achieve its objectives and meet the needs of its stakeholders.

*Any of the examples shown above would be relevant to Craster, although the second bullet would be considered a more strategic rather operational risk.*

#### Role of Boards and risk and audit committees

An organisation's board is accountable for the effectiveness of its compliance-management activities and any cases of non-compliance. In some cases, boards and individual board members may be held criminally accountable, for example via corporate manslaughter charges.

Compliance-management reviews and exception reports on any serious cases of non-compliance can provide a board with the assurance that it needs and to take action where necessary.

Where present, risk and audit committees will support the work of the board on compliance management. Their work will include looking into the detail of compliance

reviews and relevant internal audits. These committees may oversee any actions taken to address identified compliance weaknesses or areas of non-compliance.

An organisation's compliance-management policy should be reviewed and approved on a periodic basis by the board or the risk and/or audit committee if present.

### **Compliance standards**

An organisation's compliance standards are a combination of:

- compliance standards that are imposed on the organisation via laws and regulation; and
- compliance standards determined by the organisation to meet its objectives and stakeholder needs.

#### Imposed standards of compliance

The degree of compliance required for health-and-safety, environmental laws or sector regulation can vary by jurisdiction. In some jurisdictions, there may be little discretion in terms of what constitutes compliance or non-compliance; in others there may be more discretion.

An example of discretion comes from UK health and safety law, which, like some other regimes, is based on the principle of 'as low as reasonably practical' (ALARP). The key term here is 'reasonably practical' which allows an organisation to weigh up hazards against the time and money required to control them. This means that organisations have to decide for themselves what is 'reasonably practical' and what is not.

Discretion can be useful when it prevents an organisation from taking costly compliance-related actions that grossly outweigh the benefits of compliance. However, it can lead to problems where the organisation and its regulator disagree on the standards for compliance. Inflexible rules that require specific actions, irrespective of the costs involved, remove this problem but can result in excessive compliance costs.

Where an organisation has discretion in determining the nature of their compliance with laws and regulations, it is important that they decide in advance the standards they will expect for compliance. It is recommended that an organisation discusses these standards with the relevant regulatory or supervisory agency to avoid any subsequent disagreements.

*The construction industry needs to be compliant with health and safety and environmental laws and regulations. The industry has experienced many instances of deaths and severe injury and pollution of the environment. Other examples that would be relevant to suppliers in would be corporate governance and procurement / contract practices. It is not expected that candidates include these examples, and other relevant examples will be considered by the markers.*

#### Voluntary standards

An organisation will have much more discretion over the degree of compliance expected from its employees when it comes to compliance standards for internal policies and procedures, or voluntary external guidance, standards or codes of conduct.

An organisation may decide that compliance should be absolute. Alternatively, it may decide to tolerate a degree of non-compliance providing that this is reported and accepted, and a clear rationale provided. This rationale will usually be on cost-benefit grounds. Where the costs of compliance exceed the benefits, a degree of non-compliance may be accepted.

Extreme care should be taken when a degree of non-compliance is allowed. All such cases should be reported to the audit committee or board so that an organisation's directors or trustees are kept informed.

*Other examples of voluntary standards might include corporate social responsibility, diversity, inclusion – over and above that which is being required formally, for example the UK Equality Act 2010. It is not expected that candidates include these examples, and other relevant examples will be considered by the markers.*

### **Developing a compliance management framework**

To ensure that the agreed compliance standards are enforced within an organisation, three processes and controls are required:

- compliance-management policies and procedures
- compliance reporting and escalation processes
- compliance training and communication.

#### Compliance-management policies and procedures

An organisation may have a dedicated compliance-management policy. This policy should contain:

- the compliance standards and principles that are expected;
- links to key compliance-management procedures;
- reporting and escalation arrangements; and
- roles and responsibilities for the board, senior management, other managers and employees, and the risk, audit, governance and compliance functions if present.

In terms of compliance-management principles, common principles include:

- an expectation that all employees will act honestly and with integrity;
- to manage compliance risks in order to preserve the reputation and financial resources of an organisation;
- that all decision-makers own the compliance risks that are associated with the decisions that they make, even though the board is ultimately responsible for effective compliance; and
- that compliance-related risks must be monitored adequately and all cases of non-compliance escalated to the appropriate level of management.

Compliance-management procedures can be varied. Compliance-related elements may be present in operational procedures, such as procedures for operating machinery, recruiting staff or making cash transfers.

In terms of specific procedures, there may be procedures for reporting and escalation, as well as procedures for testing compliance-related controls to ensure that they are operating effectively. Other procedures include:

- how to deal with enquiries from regulators, such as who should speak with them;
- how to investigate cases of unauthorised non-compliance;
- disciplinary procedures for unauthorised non-compliance; and
- procedures for temporarily allowing non-compliance on cost-benefit grounds.

An organisation may permit a degree of non-compliance where the costs of compliance far exceed the benefits. Extreme care is needed when making such decisions. Before such a decision is made it is recommended that an organisation should discuss it with the relevant regulatory authority.

#### Compliance reporting and escalation processes

The managers and directors of an organisation will require regular assurance that it is complying with relevant laws and regulations and that any associated compliance risks are managed effectively. This assurance may come in the form of compliance reports. One common form of reporting is a periodical review of compliance. This review is normally prepared by a company secretary or governance professional and reported to the board of directors or trustees. The review will remind the board of the various laws and regulations that must be complied with and outline the various processes and controls that are in place to ensure compliance. Evidence of the effectiveness of these processes and controls may be provided, such as the results of compliance reviews and internal audits.

Compliance monitoring and reporting to management and senior management will occur much more regularly. This might include daily control-effectiveness checks to ensure that compliance with financial crime regulations is adhered to, such as the prevention of money laundering. Regular food hygiene checks or checks on health-and-safety equipment may be required, for example. Management need to know that these checks have been performed and the results of these checks, especially where non-compliance is detected.

Escalation processes come into play when ineffective controls are detected or where employees or managers are not behaving in an appropriate manner. Escalation may occur as a result of an audit finding, regular compliance-control checks, or whistleblowing. Escalation should be to the appropriate level of management. Where non-compliance threatens the whole organisation, it should be escalated to the most senior level possible, usually the board. Non-compliance that is considered to be less serious, such as a minor breach of health-and-safety rules, should be escalated to the appropriate line manager for action.

Compliance training and communication

Employees may require training to understand the importance of complying with all applicable laws and regulations and to help them operate the relevant compliance controls effectively.

This training may be provided in-house or by an external training agency. For example, health-and-safety training can be purchased from external providers, such as training on how to perform risk assessments, safe manual handling, fire or food-safety training. Regular compliance-oriented communication can supplement formal training. This might include emails or memos reminding staff of specific compliance responsibilities, poster campaigns, discussions in staff meetings, away days or awareness weeks.

*All aspects of a compliance management framework are relevant to the scenario, and will introduce more consistent and value adding compliance management to Craster, especially as the findings from the audit report showed that some key controls are not operating effectively and that there are a number of areas showing non-compliance.*

Level	Mark	Descriptor
	0	No rewardable material.
<b>Level 1 (Fail)</b>	1-12	<ul style="list-style-type: none"> <li>The answer gives an incomplete or incorrect understanding of the compliance management.</li> <li>The answer provides incomplete or incorrect information on why compliance management is important for organisations.</li> <li>The answer gives an incomplete or incorrect understanding of the responsibility of the Board in relation to compliance management.</li> </ul>

		<ul style="list-style-type: none"> <li>• The answer provides an incomplete or incorrect information on the two types of compliance standards that organisations need to adhere to, with no examples of standards provided.</li> <li>• The answer provides an incomplete or incorrect understanding of developing a compliance framework with less than four of the key components.</li> <li>• The answer makes few, if any, links between the theory and practice, using the scenario.</li> </ul>
<b>Level 2 (Pass)</b>	13-16	<ul style="list-style-type: none"> <li>• The answer provides a basic understanding of the compliance management.</li> <li>• The answer gives an overview on why compliance management is important for organisations.</li> <li>• The answer provides an overview of the of the responsibility of the Board in relation to compliance management.</li> <li>• The answer provides basic information on the two types of compliance standards that organisations need to adhere to with one example standard provided.</li> <li>• The answer provides basic information of developing a compliance framework, including the four of the key components.</li> <li>• The answer includes clear links between theory and practice, using the scenario.</li> </ul>
<b>Level 3 (Merit / Distinction)</b>	17-25	<ul style="list-style-type: none"> <li>• The answer gives a strong and comprehensive understanding of compliance management.</li> <li>• The answer illustrates a clear and strong understanding of why compliance management is important for organisations.</li> <li>• The answer gives a strong and comprehensive understanding of the responsibility of the Board in relation to compliance management.</li> <li>• The answer illustrates a clear and strong understanding of the two types of compliance standards that organisations need to adhere to with more than one example provided.</li> <li>• The answer illustrates a clear and comprehensive knowledge of developing a compliance framework, including the four key components.</li> <li>• The answer makes strong links between theory and the scenario, which is supported with appropriate examples both from the scenario and the real world.</li> </ul>

**TOTAL FOR SECTION B = 25 MARKS**  
**TOTAL FOR PAPER = 100 MARKS**

*The scenarios included here are entirely fictional. Any resemblance of the information in the scenarios to real persons or organisations, actual or perceived, is purely coincidental.*

**END**