CIMA P3 Risk Management

Mock exam: 60 questions in 90 minutes, with an answer key and explanations

How to use this mock

- Set a timer for **90 minutes** and answer every question without notes. Write your answers in the grid on the next page.
- Mark your answers using the answer key, then read the explanation for every question you got wrong or guessed.
- The questions cover every section of the syllabus, in proportion to the GoQualified question bank for P3.
- Prefer to sit it on screen? The **Exam Sim** on **goqualified.co.uk/cima/p3/** times you, marks the paper and shows your weakest section.
- All questions are original GoQualified practice questions, not past exam questions.

Free from GoQualified. Questions start on page 3; the answer key and explanations follow them. Download the latest version from goqualified.co.uk/cima/p3/.

Your answers

1 _____	13 _____	25 _____	37 _____	49 _____
2 _____	14 _____	26 _____	38 _____	50 _____
3 _____	15 _____	27 _____	39 _____	51 _____
4 _____	16 _____	28 _____	40 _____	52 _____
5 _____	17 _____	29 _____	41 _____	53 _____
6 _____	18 _____	30 _____	42 _____	54 _____
7 _____	19 _____	31 _____	43 _____	55 _____
8 _____	20 _____	32 _____	44 _____	56 _____
9 _____	21 _____	33 _____	45 _____	57 _____
10 _____	22 _____	34 _____	46 _____	58 _____
11 _____	23 _____	35 _____	47 _____	59 _____
12 _____	24 _____	36 _____	48 _____	60 _____

Questions

Question 1

What is the primary function of a risk register within an organisation's enterprise risk management process?

A To serve purely as a historical archive of risks that occurred in the past, with no ongoing use for monitoring current or emerging risks

B To replace the need for any risk appetite statement or board-level risk oversight, since a completed risk register is considered fully sufficient on its own

C To document only risks that have already resulted in a financial loss, excluding any risk that has not yet caused measurable financial harm

D To provide a structured, documented record of identified risks, their assessed likelihood and impact, ownership, and the status of mitigating actions, supporting ongoing monitoring and accountability

Question 2

ISO 31000:2018 sets out a widely referenced set of risk management principles and a generic risk management process. What is the primary purpose of this international standard?

A To mandate a single, legally binding risk management process that every organisation, regardless of size, sector or jurisdiction, must adopt without any adaptation

B To apply exclusively to financial services organisations, since ISO 31000 was developed specifically and solely for banks and insurance companies

C To provide generic guidelines and principles for effective risk management applicable across different types of organisation, rather than prescribing risk management activity specific to one industry or one particular type of risk

D To replace the need for any organisation-specific risk appetite statement, since ISO 31000 itself defines a universal risk appetite applicable to every organisation

Question 3

The COSO ERM framework (2017) identifies governance and culture as one of its five interrelated components, placed foundationally within the framework. What does this positioning suggest about the framework's view of how effective enterprise risk management is actually achieved?

A Governance and culture are treated as entirely peripheral, optional add-ons within the COSO ERM framework, with no meaningful bearing on how effectively the other four components actually operate

B The COSO ERM framework treats governance and culture as relevant only to publicly listed companies, with no application to privately held or smaller organisations

C Effective ERM depends significantly on the tone set by governance and organisational culture, which shapes how the other framework components are actually put into practice

D Governance and culture is defined within COSO ERM 2017 as being concerned exclusively with formal board meeting frequency, with no broader meaning beyond this narrow procedural point

Question 4

A company identifies a low-probability, low-impact risk where the cost of any mitigation would clearly exceed the risk's expected financial consequence. Which TARA response is most appropriate, and why?

A Avoid — since any identified risk, however minor, should always be eliminated by ceasing the associated activity entirely

B Transfer — since insurance should always be purchased for every risk regardless of its probability, impact, or the cost of the premium relative to the risk

C Reduce — since every risk must always be actively mitigated to some extent, regardless of whether the cost of doing so exceeds the risk's expected impact

D Accept — since the cost of mitigation would exceed the expected impact, consciously retaining the risk without further action is the economically rational response

Question 5

Within the COSO ERM framework's performance component, why is it considered important to assess actual performance in relation to the level of risk that was taken to achieve it, rather than evaluating performance results in isolation?

A Evaluating performance alongside the risk taken provides a fuller picture, since strong results from excessive risk may be less desirable than modest results within acceptable risk boundaries

B Performance should always be evaluated entirely independently of any risk consideration, since risk and performance are treated as completely unrelated concepts within COSO ERM

C Only performance results matter for evaluation purposes; the level of risk taken to achieve any given result is characterised as strategically and managerially irrelevant

D Risk-adjusted performance evaluation is relevant only to financial services organisations, with no application to organisations in other sectors of the economy

Question 6

Why does COSO ERM emphasise considering risk as an integral part of setting strategic objectives, rather than setting objectives first and only considering risk afterward as a separate step?

A Considering risk during objective-setting helps ensure objectives are realistic given the organisation's risk appetite, rather than discovering unacceptable risk only later

B Risk should always be considered only after objectives have been finalised, since considering risk during objective-setting would make the objectives themselves overly cautious and unambitious

C Risk and objective-setting are entirely separate, unconnected processes with no meaningful relationship between how objectives are chosen and what risks they might create

D COSO ERM does not address objective-setting at all, focusing exclusively on managing risks to objectives that have already been set by some other, unrelated process

Question 7

Why does COSO ERM include 'review and revision' as one of its five components, rather than treating the initial design of the ERM framework as a one-time exercise?

A Review and revision is concerned exclusively with reviewing the wording of the organisation's mission statement, with no broader connection to the effectiveness of the risk management framework itself

B An ERM framework, once properly designed, is treated as permanently effective and complete, requiring no subsequent review or adjustment under any future circumstances

C Review and revision applies only to very large organisations undertaking major transformation programmes, and has no relevance to organisations of a more typical size or stability

D Review and revision recognises that risk exposures, the business environment, and organisational objectives all change over time, meaning the ERM framework itself needs periodic reassessment and adjustment to remain effective and relevant

Question 8

A board evaluates two strategic options: one offers modest but highly certain returns, the other offers potentially much higher returns but with significantly greater uncertainty. How should the board's documented risk appetite inform this choice, and why is this connection important?

A Risk appetite mainly serves as a retrospective benchmark for reviewing past decisions, rather than something that should actively shape which option the board selects going forward

B The board should always select the option with the potentially higher return, regardless of its own documented risk appetite or the greater uncertainty involved

C Risk appetite is primarily a tool for guiding operational risk-taking decisions, with strategic choices at board level generally guided by other considerations instead

D The board's documented risk appetite should directly inform which option is more consistent with the risk it has stated it is willing to accept, not made in isolation from that

Question 9

A modern view of enterprise risk management recognises that risk can present both downside threats and upside opportunities. How does incorporating this broader view change how an organisation might approach ERM compared with a purely defensive, loss-prevention-focused view?

A ERM should always focus exclusively on downside threats, since considering any upside or opportunity dimension is treated as entirely outside the legitimate scope of enterprise risk management

B Upside risk and downside risk are simply two different names for exactly the same concept, with no meaningful distinction between them in modern ERM thinking

C Incorporating upside risk means ERM also considers how the organisation can position itself to capture favourable, unexpected opportunities, not solely how to defend against and minimise adverse outcomes

D Considering upside risk within ERM guarantees that an organisation will always achieve better financial performance than one that focuses solely on downside protection

Question 10

A board recognises that none of its current members has deep specialist expertise in a particular emerging risk area (such as advanced cyber threats), and engages an external specialist to brief the board periodically on developments in this area. What does this practice illustrate about effective board risk oversight?

A Effective board risk oversight can involve recognising genuine gaps in specialist knowledge and proactively supplementing it with external expertise, rather than assuming general experience is always sufficient

B No practice of value is illustrated here, since engaging external specialists is generally considered to be always unnecessary if a board already has general business experience, regardless of any specific specialist knowledge gap

C Boards should never seek external expertise on any risk topic, since doing so is understood to be an implicit admission that the board itself is fundamentally inadequate to its role

D This practice is worthwhile only once a formal risk committee has already been established, and offers little value to a board without one in place

Question 11

A seemingly minor operational risk in one part of an organisation (a delayed IT system upgrade) turns out, when examined holistically, to also increase cyber risk (running on an unsupported, unpatched system), reputational risk (potential customer-facing service issues), and compliance risk (potentially failing a specific regulatory requirement tied to system capability). What does this scenario illustrate about the value of an enterprise-wide, rather than siloed, view of risk?

A No value exists in an enterprise-wide view of risk at all, since each risk category (operational, cyber, reputational, compliance) is characterised as entirely independent with no possible connection between them in any organisation

B A siloed, department-by-department approach to risk management is always superior to an enterprise-wide view, since siloed management is generally considered to be inherently more thorough within each individual specialist area

C An enterprise-wide view can reveal how a single underlying issue can create compounding, interconnected risk across multiple categories simultaneously, a connection that siloed, department-by-department risk management would likely miss by considering each risk category in isolation

D This kind of interconnected risk pattern can only ever arise in very large, complex organisations, and never arises in smaller organisations with simpler operational structures

Question 12

A board treats a single positive internal audit opinion on a specific process as complete, permanent assurance that no further risk exists in that area, with no further monitoring considered necessary. What limitation does this reliance illustrate?

A No limitation exists at all, since a single positive internal audit opinion is typically viewed as providing permanent, unconditional assurance that no further risk can ever arise in that area again

B A single audit opinion reflects conditions at a point in time and doesn't guarantee continued effectiveness afterward, so ongoing monitoring remains necessary since circumstances can change

C Internal audit opinions should never be relied upon at all for any purpose, since they are defined as providing no genuine assurance value whatsoever under any circumstances

D This limitation applies only to internal audit specifically, and never applies to any other form of assurance such as external audit opinions

Question 13

An organisation believes risk management is solely the job of its dedicated risk department, with line managers and staff elsewhere treating risk-related concerns as entirely someone else's responsibility. What limitation does this belief illustrate about effective ERM?

A No limitation exists at all, since a dedicated risk department is treated as always fully capable of identifying and managing every organisational risk without any input or awareness needed from line managers or other staff

B Risk management should always be performed exclusively by the board, with no meaningful role for either a dedicated risk department or line management in identifying or managing risk

C This belief reflects best practice, since concentrating all risk responsibility in a single specialist department is regarded as inherently more effective than distributing risk awareness across the organisation

D Effective ERM depends on risk awareness and responsibility being genuinely shared across the organisation, not confined to a specialist risk department alone, since risks often first become visible to those closest to day-to-day operations, not to a centralised specialist function

Question 14

A board sets a risk tolerance limit stating that no single identified risk should be capable of causing a loss exceeding 3% of the organisation's net assets. The organisation's net assets are $200 million. What is the maximum loss, in $ million, that a single risk can threaten before it breaches this tolerance limit?

A 3

B 6

C 60

D 200

Question 15

As a simple way of relating performance to the risk taken to achieve it, a division reports a return of 12% for the year, achieved with a measured risk (volatility) of 8%. What is the resulting risk-adjusted performance ratio, to one decimal place?

A 0.7

B 1.5

C 4.0

D 96.0

Question 16

A company continues operating an established business model that has generated reliable profits for many years, even as clear signals emerge that customer needs and the competitive landscape are shifting in ways the current model is poorly suited to serve. What strategic risk does persisting with an increasingly outdated business model illustrate, and what condition tends to make this risk particularly dangerous?

A Financial risk, since the scenario concerns exclusively the calculation of specific financial ratios rather than any consideration of the broader business model itself

B Limited risk, since a business model that has generated reliable profits for many years is generally a strong predictor that it remains well suited to the current market for the foreseeable future

C Cyber risk, since the scenario describes a threat originating specifically from a digital or information security source rather than from broader shifts in the market

D Business model obsolescence risk — particularly dangerous since reliable current profits can create a false sense of security, delaying adaptation until relevance has already eroded

Question 17

A company's strategy was built on the assumption that a key trading partner's political and economic stability would remain constant, but that partner has since experienced significant instability, disrupting the company's supply chain and market access. What does this scenario illustrate about the nature of strategic risk?

A Strategic risk can arise when a key assumption underlying the strategy is invalidated by real-world events, highlighting the need to periodically test such assumptions

B This scenario illustrates no strategic risk whatsoever, since political and economic events in another country are defined as entirely outside the scope of any organisation's own strategic risk considerations

C Strategic assumptions, once made at the time a strategy is initially developed, should never be revisited or tested again for the entire remaining life of that strategy

D This type of disruption can only ever affect very small organisations with limited resources, and never affects large, well-resourced multinational companies

Question 18

A company enters a strategic alliance with a partner whose long-term interests, once revealed more fully over time, prove to diverge significantly from the company's own strategic direction, creating friction and undermining the alliance's original objectives. What strategic risk does this scenario illustrate, and what practice might help mitigate it in future alliance decisions?

A Minimal risk, provided both alliance partners signed a formal partnership agreement at the outset, since a signed agreement is generally sufficient on its own to guarantee ongoing strategic alignment

B Operational risk exclusively, since any difficulty within an alliance is best understood purely in terms of day-to-day operational execution rather than the strategic direction of the partnership

C Reputational risk exclusively, since the visible friction between alliance partners is best understood only in terms of how it might be perceived externally, rather than any effect on the alliance's own strategic objectives

D Partner alignment risk within strategic alliances — thorough due diligence on a prospective partner's genuine long-term strategic interests and objectives before committing to an alliance can help identify potential misalignment earlier

Question 19

A company's core product relies on a specific underlying technology that a faster-improving alternative technology could plausibly render obsolete within the coming years. What strategic risk does this scenario illustrate, and why might monitoring this risk be particularly challenging?

A No risk exists at all, since a company's core underlying technology, once established and successful, can never become obsolete under any future circumstances

B Technology obsolescence risk — challenging to monitor because the pace and success of an emerging alternative technology are genuinely uncertain, making timing hard to predict

C Cyber risk exclusively, since any risk relating to technology of any kind is automatically treated as a reputational risk rather than a broader strategic risk category

D Financial risk exclusively, since technology obsolescence can only ever be meaningfully analysed and understood using narrow financial statement metrics

Question 20

A company continues investing heavily in expanding capacity for a product category whose underlying customer demand has been steadily declining for several years due to a genuine, sustained shift in consumer preferences. What strategic risk does this scenario most directly illustrate?

A No strategic risk exists at all, since continuing to invest in an existing, previously successful product category is always the objectively correct strategic decision regardless of any subsequent evidence about changing demand

B Cyber risk, since any risk relating to customer behaviour of any kind is automatically treated as a compliance matter rather than a broader strategic risk category

C The risk of misjudging a genuine, sustained shift in customer preferences, continuing to invest in declining demand rather than reallocating towards growing interest

D Regulatory risk exclusively, since changes in customer preference can only ever occur as a direct consequence of new government regulation being introduced

Question 21

A company's competitive position depends heavily on the expertise and relationships of a small number of key senior individuals, with no documented succession plan or knowledge transfer process in place. What strategic risk does this illustrate, and what practice could help mitigate it?

A No risk exists at all, since relying on a small number of highly capable senior individuals is always the safest possible organisational structure regardless of any succession considerations

B Cyber risk, since any risk relating to individual employees is automatically treated as an operational risk rather than a broader strategic risk category

C Financial risk exclusively, since key person dependency can only ever be understood and analysed using narrow financial statement metrics

D Key person dependency risk — succession planning and deliberate knowledge transfer processes can help reduce the organisation's vulnerability to the sudden loss of these critical individuals

Question 22

A company faces growing pressure from investors, customers and regulators regarding its environmental impact, but has not integrated environmental considerations into its core strategic planning process. What strategic risk does this gap illustrate, and why is it increasingly significant?

A No risk exists at all, since environmental considerations are defined as entirely irrelevant to any organisation's core strategic planning process regardless of industry or stakeholder pressure

B ESG-related strategic risk — failing to integrate environmental considerations into strategic planning can expose the company to investor pressure, shifting customer preferences, and regulatory consequences

C Cyber risk, since any risk relating to external stakeholder pressure of any kind is automatically treated as a purely financial risk rather than a broader strategic risk category

D Financial risk exclusively, since ESG-related pressures can only ever be understood and analysed using narrow financial statement metrics with no broader strategic dimension

Question 23

A company's strategic plan assumes continued low interest rates and stable inflation over the coming years, with no contingency built in for a significant change in macroeconomic conditions. What strategic risk does this scenario illustrate, and what practice might help address it?

A No risk exists at all, since interest rates and inflation are defined as permanently stable factors that never meaningfully change over any multi-year strategic planning period

B Cyber risk, since any risk relating to macroeconomic conditions of any kind is automatically treated as a reputational risk rather than a broader strategic risk category

C Macroeconomic risk arising from an inflexible plan built on a single set of economic assumptions — incorporating scenario analysis or contingency planning for alternative macroeconomic conditions can help build greater strategic resilience

D Reputational risk exclusively, since changes in macroeconomic conditions can only ever affect an organisation's external public image and have no other strategic consequence

Question 24

A company's strategic planning process focuses almost exclusively on well-established, currently visible competitors and trends, with no formal process for scanning for weaker, more distant signals of emerging change that could become significant in future. What limitation does this narrow strategic risk monitoring approach illustrate?

A No limitation exists at all, since focusing exclusively on currently visible, well-established competitors and trends is always fully sufficient for effective strategic risk monitoring in every context

B Horizon scanning for weaker or more distant emerging signals is a completely worthless activity that has never once identified any strategically significant trend in practice

C Formal horizon scanning only becomes worthwhile once a company has expanded into several overseas markets, and offers little value while it remains focused on a single domestic market

D The organisation risks being caught unprepared by emerging strategic threats or opportunities that a more deliberate, formal horizon-scanning process might have identified at an earlier, more addressable stage

Question 25

A company relies on a single production facility for the entire output of its most important product line, with no alternative production capability elsewhere. What strategic risk does this illustrate, and what general approach could help address it?

A No risk exists at all, since relying on a single production facility is always the most efficient and lowest-risk approach for any organisation regardless of that facility's importance to overall output

B Single point of failure risk — a significant disruption to that one facility (fire, natural disaster, equipment failure) could halt the entire product line's output; developing alternative or backup production capability can help reduce this concentrated vulnerability

C Cyber risk exclusively, since any risk relating to a physical production facility is automatically treated as an operational risk rather than a broader strategic or operational risk category

D This risk can only ever apply to very small organisations with limited capital, and never applies to large, well-capitalised organisations with substantial production facilities

Question 26

A management team characterises a series of unreviewed, incremental departures from the organisation's original strategy as 'deliberate adaptive flexibility', when in reality no genuine strategic reassessment has actually taken place at any point. What risk does this mischaracterisation illustrate?

A Limited risk, since a management team's own confidence in characterising a pattern of change as deliberate adaptation is usually a reliable indicator that genuine strategic reassessment has, in substance, taken place

B The risk that genuine strategic drift is mislabelled as intentional adaptation, masking the fact that no real strategic reassessment has occurred and potentially delaying the kind of genuine review that would catch a real problem

C Operational risk exclusively, since how a management team internally describes a pattern of change is best understood as a communications or reporting matter rather than a genuine strategic concern

D This mischaracterisation is most likely in organisations with very formal, well-documented strategic planning processes, since extensive documentation can make incremental changes easier to relabel retrospectively as deliberate

Question 27

A company's core customer base is concentrated in an age demographic that is shrinking as a proportion of the overall population, while the company has made no strategic effort to also appeal to growing younger demographic segments. What strategic risk does this illustrate?

A No risk exists at all, since demographic trends in the overall population are defined as having no bearing whatsoever on any individual company's customer base or strategic position

B Cyber risk, since any risk relating to customer demographics is automatically treated as a compliance matter rather than a broader strategic risk category

C Demographic concentration risk — reliance on a shrinking segment without a strategy for growing segments risks a gradually eroding customer base as the population structure shifts

D This risk can only ever affect companies in the retail sector specifically, and never affects companies operating in any other industry

Question 28

A company has no formal crisis management plan or trained crisis response team, believing that a genuine major crisis is unlikely enough that dedicated preparation is unnecessary. What strategic risk does this lack of preparation illustrate?

A No risk exists at all, since a major crisis is understood to be so unlikely for any organisation that dedicated crisis management preparation is never a worthwhile use of organisational resources

B Cyber risk exclusively, since any risk relating to organisational crisis preparedness is automatically treated as an operational risk rather than a broader strategic risk category

C This risk can only ever apply to very large organisations operating in high-risk industries, and never applies to smaller organisations or those in lower-risk industries

D The risk of inadequate crisis response capability — without prior planning, an organisation facing a major crisis is likely to respond more slowly and less effectively than one that prepared in advance

Question 29

A company consistently invests a smaller proportion of revenue in research and innovation than its main competitors, prioritising short-term margin preservation instead. What strategic risk does this pattern illustrate over the longer term?

A No risk exists at all, since prioritising short-term margin preservation over innovation investment is always the objectively correct strategic choice regardless of competitors' relative innovation investment levels

B Innovation underinvestment risk — persistently under-investing relative to competitors risks a gradual erosion of competitive position as rivals develop superior products the company can't match

C Cyber risk, since any risk relating to research and innovation investment levels is automatically treated as a compliance matter rather than a broader strategic risk category

D This risk can only ever affect companies in fast-moving technology sectors, and never affects companies in more traditional or slower-moving industries

Question 30

A company is considering entering a new overseas market. Management estimates a 60% probability of achieving a profit of £5 million if the entry succeeds, and a 40% probability of incurring a loss of £1 million if it does not. What is the expected value of this market entry decision?

A £3,000,000

B £2,600,000

C £3,400,000

D £4,000,000

Question 31

How do inherent risk, control risk and detection risk relate to one another in the context of assessing the risk of a material error or issue going unaddressed?

A Inherent risk = susceptibility before controls; control risk = controls fail to catch it; detection risk = review also fails — all three combine

B Inherent risk, control risk and detection risk are simply three different names for exactly the same underlying concept, with no meaningful distinction drawn between them

C Detection risk refers to the susceptibility to error before considering controls, while inherent risk refers to the risk that review procedures fail to identify an existing error

D Only inherent risk is ever relevant to assessing the overall risk of an issue going unaddressed, with control risk and detection risk defined as having no bearing on this overall assessment

Question 32

An internal audit function conducts a review specifically assessing whether the organisation's operations comply with a specific set of external regulatory requirements. What type of internal audit engagement does this represent, as distinct from a value-for-money or fraud-focused audit?

A A value-for-money audit, since any internal audit engagement assessing any aspect of organisational operations is automatically classified as a value-for-money audit regardless of its actual specific focus

B A fraud audit, since compliance with regulatory requirements is regarded as identical in scope and purpose to investigating suspected fraudulent activity

C A compliance audit — assessing adherence to specific external regulatory or internal policy requirements, distinct from a value-for-money audit or a fraud audit

D There is no meaningful distinction between different types of internal audit engagement, since internal audit is characterised as performing exactly the same single type of review in every engagement

Question 33

Why is it generally considered important for an internal audit function to report administratively and functionally to a level of the organisation independent of the specific operations it audits, such as to the audit committee rather than to the manager whose department is being audited?

A Internal audit's reporting line has no bearing whatsoever on the objectivity or credibility of its findings, regardless of which level of the organisation it reports to

B Internal audit should always report directly to the specific manager whose department is being audited, since this reporting line is generally considered to be producing the most objective and useful findings

C Internal audit independence is relevant only in very large multinational organisations, with no meaningful application to the internal audit function of a smaller organisation

D Reporting to an independent level helps preserve the internal audit function's objectivity, reducing the risk that findings are influenced or suppressed by the very management whose performance and controls are being assessed

Question 34

Within the COSO Internal Control framework's control environment component, why is 'tone at the top' considered such a significant influence on the overall effectiveness of an organisation's internal control system?

A Tone at the top refers exclusively to the specific font and visual formatting used in an organisation's written internal control policy documents, with no broader behavioural meaning

B Senior leadership's demonstrated commitment to integrity significantly influences how seriously controls are taken elsewhere, since employees take cues from observed behaviour, not just stated policy

C Senior leadership behaviour has no meaningful influence whatsoever on how internal controls are actually followed and applied elsewhere in the organisation, regardless of what that behaviour demonstrates

D Tone at the top is relevant only to how external auditors are greeted during their annual visit, with no broader relevance to internal control effectiveness throughout the year

Question 35

A value-for-money (VFM) audit is typically structured around assessing three related dimensions of an organisation's use of resources. What are these three dimensions?

A Revenue, cost and profit, since value-for-money audits are defined as assessing only these three narrow financial statement measures

B Compliance, fraud and cybersecurity, since these three areas are defined as constituting the complete scope of any value-for-money audit

C Economy (acquiring resources at appropriate cost and quality), efficiency (converting inputs to outputs with minimal waste), and effectiveness (achieving intended outcomes and objectives)

D Governance, culture and reputation, with no consideration given to how resources are actually acquired, converted or used to achieve outcomes

Question 36

An internal audit function has limited resources and cannot audit every area of the organisation every year. What approach is generally considered best practice for prioritising which areas to audit, and why?

A An approach that audits every department in strict alphabetical order each year, regardless of each department's actual assessed risk level or significance to the organisation

B An approach that audits only the departments senior management personally prefers to have reviewed, regardless of any independent assessment of comparative risk across the organisation

C A risk-based approach, prioritising audit coverage towards the areas assessed as carrying the greatest risk to the organisation's objectives, making the most effective use of limited audit resources

D An approach that never revisits any previously audited area, regardless of how significant or high-risk that area may currently be assessed as being

Question 37

An internal audit team identifies significant control weaknesses and makes clear recommendations, but the audit function has no formal process for tracking whether management actually implements those recommendations afterward. What limitation does this gap illustrate?

A No limitation exists at all, since simply identifying and formally reporting a control weakness always automatically results in that weakness being fixed by management without any need for further follow-up

B Internal audit's responsibility ends entirely and completely once a report is issued, meaning any subsequent follow-up on recommendations is inherently outside the legitimate scope of the internal audit function

C Without a formal follow-up process, there is a risk that identified control weaknesses remain unaddressed despite being identified, undermining the practical value of the audit work performed, since identification alone does not itself fix the underlying weakness

D Tracking whether recommendations have been implemented is a task that should always be performed by external audit exclusively, with no role for internal audit itself in this follow-up process

Question 38

Even a well-designed and properly operating system of internal control cannot provide absolute assurance against error or fraud. What inherent limitations of internal control does this reflect?

A No inherent limitations exist at all, since a sufficiently well-designed system of internal control is typically viewed as capable of providing complete, absolute assurance against all error and fraud without any exception

B The only inherent limitation of internal control is inadequate staff training, with no other factor capable of ever limiting the effectiveness of even a well-designed control system

C Internal control limitations apply only to smaller organisations with fewer resources, and do not apply in any meaningful way to large, well-resourced organisations with sophisticated control systems

D Inherent limitations include human error, collusion, management override, and cost-benefit design trade-offs

Question 39

COSO's monitoring activities component distinguishes between 'ongoing evaluations' built into normal business processes and 'separate evaluations' conducted periodically. What is the difference between these two, and why might an organisation use both?

A Ongoing evaluations give real-time visibility; separate evaluations give periodic independent depth — using both is complementary

B Ongoing evaluations and separate evaluations are simply two different names for exactly the same monitoring activity, with no meaningful distinction between them

C Separate evaluations are built into day-to-day operations, while ongoing evaluations are conducted periodically through internal audit, reversing the standard terminology

D An organisation should only ever use one of these two types of evaluation, since using both simultaneously is characterised as inherently duplicative and wasteful

Question 40

An organisation maintains a formal delegated authority matrix specifying which level of management must approve transactions or decisions above specified value thresholds. What control purpose does this matrix serve, and what risk arises if it is not consistently followed in practice?

A The matrix serves no genuine control purpose at all, since delegated authority documentation is typically viewed as a purely administrative formality with no bearing on actual decision quality or oversight

B If the matrix is not consistently followed, this always and exclusively indicates deliberate fraud, with no other possible explanation for any departure from the documented thresholds

C A delegated authority matrix is needed only where board members actively disagree with one another, and serves no real purpose where the board is in full agreement

D It ensures decisions of a given significance get appropriately senior scrutiny; if not followed, decisions may be approved at too junior a level, undermining oversight

Question 41

COSO's Internal Control—Integrated Framework addresses internal control in relation to three broad categories of organisational objectives: operations, reporting, and compliance. Why is it important that internal control addresses all three categories, rather than focusing solely on financial reporting objectives?

A COSO's Internal Control—Integrated Framework is concerned exclusively with financial reporting objectives, with operations and compliance defined as entirely outside its scope

B Operational and compliance objectives are always automatically and fully achieved once financial reporting objectives have been satisfied, requiring no separate internal control consideration

C Weaknesses can affect operations and compliance too, not just financial reporting — a narrow focus would miss these risks

D Internal control addressing operational and compliance objectives is relevant only to organisations operating in heavily regulated industries, with no relevance to organisations in less regulated sectors

Question 42

An organisation outsources its payroll processing to a third-party service provider, but performs no independent monitoring or periodic assurance review of that provider's own control environment, effectively assuming the provider's processes must be adequately controlled without verification. What control weakness does this illustrate?

A No control weakness exists at all, since outsourcing any process to a third-party provider always and automatically transfers full responsibility for control adequacy entirely away from the outsourcing organisation

B This scenario illustrates strong internal control, since assuming a third-party provider's processes are adequately controlled without any verification is treated as an efficient and sufficient control approach

C Inadequate oversight of outsourced processes — outsourcing doesn't eliminate the organisation's own responsibility for ensuring adequate control exists, so ongoing monitoring or periodic independent assurance remains important

D Controls over outsourced processes are needed only where the service provider is based overseas, and are unnecessary where the provider operates in the same country as the organisation

Question 43

An internal audit report contains technically accurate findings but is written in dense, highly technical language that senior management and the audit committee find difficult to interpret and act upon. What limitation does this illustrate about the value of internal audit work, and what does it suggest about effective audit reporting?

A Technically accurate findings provide limited value if not communicated clearly enough for the audience to act on, so effective reporting needs clear, accessible communication, not accuracy alone

B No limitation exists at all, since the technical accuracy of audit findings is typically viewed as the only factor that matters for effective audit reporting, regardless of how clearly or accessibly those findings are actually communicated

C Audit reports should always be written in the most technical language possible, since accessibility to a non-specialist audience is treated as an inappropriate compromise of proper audit rigor

D Communication clarity is relevant only for audit reports directed at very senior audiences such as the full board, and has no relevance to reports directed at operational management

Question 44

A proposed control costs £20,000 per year to operate. Without the control, the expected loss from a particular error is 20% probability x £300,000 impact = £60,000 per year. With the control in place, the probability of the error occurring falls to 5%, giving an expected loss of £15,000 per year. What is the net annual benefit of implementing the control?

A £45,000
B £20,000
C £25,000
D £60,000

Question 45

An internal audit team sets a materiality threshold at 2% of total assets for the purposes of a specific review. The organisation's total assets are £8 million. What is the resulting materiality threshold?

A £80,000
B £16,000
C £160,000
D £800,000

Question 46

An organisation's systems are infected with software that encrypts critical files and demands payment before decryption keys are provided. What type of malware does this represent, and what does this attack primarily target?

A Ransomware — it primarily targets the availability of data and systems, denying the organisation access to its own information until a ransom demand is met (or the data is otherwise recovered)
B A virus, since ransomware and viruses are defined as exactly the same type of malware with no meaningful distinction between them
C Spyware, since encrypting files and demanding payment is treated as identical in mechanism and objective to covertly monitoring user activity without their knowledge
D A firewall exploit, since ransomware is regarded as a vulnerability in network firewall configuration rather than a distinct category of malicious software

Question 47

What is the primary purpose of the ISO 27001 standard in relation to an organisation's approach to cybersecurity and information security?

A It provides a purely technical specification for firewall hardware configuration, with no consideration of organisational processes, policies or people-related security factors
B It applies only to government organisations, with no relevance or applicability to private-sector companies of any kind
C It mandates that every certified organisation must use one single, identical, prescribed cybersecurity software product, regardless of the organisation's specific circumstances or risk profile
D It provides a framework and set of requirements for establishing, implementing, maintaining and continually improving an information security management system, covering people, processes and technology, not solely technical controls

Question 48

An organisation delays applying a security patch released by its software vendor for a known vulnerability, since applying it would require scheduling system downtime that is administratively inconvenient. What risk does this delay create, and why is timely patch management considered an important control?

A No risk exists at all, since a vulnerability already publicly disclosed by the vendor is no longer a genuine security concern for any organisation

B Patch management can safely be deferred indefinitely provided no known exploit has yet been publicly reported for the specific software version in use

C The delay leaves a known, publicly disclosed vulnerability unaddressed, creating a window attackers could exploit; timely patch management closes this window as quickly as practical

D Applying security patches always introduces more risk to an organisation than leaving the original known vulnerability completely unaddressed

Question 49

A disgruntled employee with legitimate system access deliberately exports and leaks confidential customer data before resigning. Why is this category of risk — insider threat — often considered particularly challenging to defend against compared with external attacks?

A Insider threat is not a genuine risk category at all, since employees with legitimate access are defined as incapable of causing any harm to the organisation

B Insider threat can only ever be addressed through firewall configuration, with no other type of control capable of providing any meaningful mitigation

C Insider threat is relevant only to very small organisations with few employees, and has no meaningful application to large organisations with extensive workforces

D Insiders already possess legitimate access and knowledge of the organisation's systems and data, meaning many external-facing technical defences (such as firewalls) are not designed to prevent this kind of authorised-access misuse

Question 50

An employee downloads what appears to be a legitimate free software utility, which secretly installs malicious code onto their computer once run. What type of malware does this represent, and how does it typically differ from a self-replicating virus?

A A Trojan disguises itself as legitimate software to trick installation; a virus self-replicates without needing to disguise itself

B A Trojan and a virus are simply two different names for exactly the same type of malware, with no meaningful distinction between how each actually operates

C Ransomware, since any malicious software delivered via a downloaded file is automatically classified as ransomware regardless of its actual specific mechanism and objective

D A firewall vulnerability, since a Trojan is treated as a network configuration weakness rather than a distinct category of malicious software

Question 51

An organisation requires employees to provide both a password and a one-time code generated by a separate authenticator app before accessing sensitive systems. What control does this represent, and why is it generally considered more effective than a password alone?

A A physical control exclusively, since any authentication process involving a mobile device is automatically and solely classified within the physical controls category with no other classification possible

B Multi-factor authentication — requiring an additional, independent factor beyond a password means that a compromised password alone is insufficient for an attacker to gain access, since they would also need the second factor

C A detective control exclusively, since multi-factor authentication is regarded as operating only after a security incident has already occurred, with no preventive function whatsoever

D A control providing no meaningful additional security benefit compared with a password alone, since any additional authentication step is characterised as purely a user inconvenience with no genuine risk-reduction value

Question 52

An organisation conducts thorough cybersecurity due diligence and monitoring of its own systems, but grants a third-party software vendor privileged access to its network for maintenance purposes, without applying similar scrutiny to that vendor's own security practices. What cyber risk does this scenario illustrate, and what practice could help address it?

A No risk exists at all, since granting privileged network access to a third-party vendor for maintenance purposes is generally considered to have no bearing whatsoever on the organisation's own overall cybersecurity exposure

B This is exclusively a contractual, legal matter with no genuine cybersecurity dimension, meaning no technical or security-focused practice is relevant to addressing it

C Supply chain / third-party cyber risk — extending due diligence and security requirements to third parties with system access helps close this gap, since strong internal security can be undermined by a less secure connected third party

D Third-party cyber risk only becomes a genuine concern once a vendor has actually suffered a breach in the past, and is not meaningful for a vendor with a clean prior track record

Question 53

Information security is commonly described in terms of three core elements, often referred to by the acronym 'CIA'. What are these three elements?

A Cost, Investment and Audit, since the CIA acronym in information security is understood to be referring to these three financial and audit-related concepts

B Compliance, Insurance and Assurance, since the CIA acronym in information security is typically viewed as referring to these three governance-related concepts

C Confidentiality is the only genuine element of information security, with Integrity and Availability defined as having no independent relevance to the field

D Confidentiality (preventing unauthorised access), Integrity (ensuring information is accurate and unaltered), and Availability (ensuring authorised access when needed)

Question 54

An organisation has invested significantly in preventive cybersecurity controls but has no documented incident response plan describing how it would actually respond if a significant cyber incident nonetheless occurred. What gap does this illustrate, and why is incident response planning considered important even alongside strong preventive controls?

A No gap exists at all, since sufficiently strong preventive controls are defined as making the occurrence of any cyber incident completely impossible, removing any need for incident response planning

B Preventive controls cannot guarantee no incident ever occurs; a tested response plan enables faster, more coordinated response

C Incident response planning is only relevant after a cyber incident has already occurred, meaning developing a plan in advance of any incident provides no genuine benefit whatsoever

D Incident response is solely the IT department's responsibility, so no organisation-wide plan is needed provided IT staff know what to do

Question 55

A vulnerability in widely used software is discovered and actively exploited by attackers before the software vendor is even aware of it, meaning no patch yet exists. What is this type of vulnerability called, and why is it particularly challenging to defend against?

A A known vulnerability, since zero-day vulnerabilities are defined as identical to any vulnerability for which a patch has already been available for an extended period

B A physical security weakness, since zero-day vulnerabilities are defined as concerning physical access to a facility rather than a software or systems weakness

C A control that organisations should never attempt to defend against, since zero-day vulnerabilities are defined as entirely unavoidable and impossible to mitigate in any way

D A zero-day vulnerability — no patch exists yet, so organisations must rely on monitoring and broader defences, not patching alone

Question 56

Many data protection regulatory regimes require organisations to notify a relevant regulator, and in some cases affected individuals, within a specified timeframe after becoming aware of a significant data breach. Why does this kind of mandatory notification requirement matter for an organisation's cyber incident response planning?

A Mandatory notification requirements have no bearing whatsoever on how an organisation should plan its incident response, since notification is characterised as an entirely separate legal matter unconnected to operational incident response

B Incident response plans need to explicitly incorporate awareness of applicable notification deadlines and requirements, since failing to notify within the required timeframe can itself result in additional regulatory penalties on top of any consequences of the breach itself

C Notification requirements apply only to organisations operating in the technology sector specifically, with no relevance to organisations in any other industry that may hold personal data

D Once a data breach has occurred, there is no benefit to planning for notification requirements in advance, since notification can only ever be properly considered after the incident has already been fully resolved

Question 57

An organisation divides its network into separate segments, so that a compromise of one segment (such as a guest Wi-Fi network) does not automatically grant an attacker access to other, more sensitive segments (such as the finance system network). What control does this represent, and what benefit does it provide in the event of a successful attack?

A A physical control exclusively, since dividing a network into segments is treated as identical to restricting physical access to a building, with no distinct technical network security dimension

B Network segmentation — it limits the potential spread and impact of a successful compromise by containing it within the affected segment, rather than allowing an attacker who breaches one part of the network to move freely across the entire network to reach more sensitive systems

C An authorisation control, since network segmentation is regarded as functioning identically to requiring senior management sign-off before a specific financial transaction is processed

D A control providing no genuine security benefit, since network segmentation is characterised as having no effect whatsoever on how far an attacker can move once any part of the network has been compromised

Question 58

Rather than attacking a target organisation directly, an attacker instead compromises a third-party website that employees of the target organisation are known to visit regularly, infecting that website so that visitors from the target organisation become infected when they visit it. What attack technique does this illustrate?

A A denial-of-service attack, since any attack ultimately affecting website visitors is automatically classified as denial-of-service regardless of its actual specific mechanism and objective

B A watering hole attack — compromising a website frequented by the intended target group, rather than attacking the target directly, exploiting the trust the target places in a familiar, regularly visited site

C Ransomware, since compromising a third-party website is understood to be functionally identical to encrypting files and demanding a ransom payment directly from the target organisation

D SQL injection exclusively, since compromising any website is automatically and solely classified as SQL injection regardless of the actual specific technique used to compromise it

Question 59

An employee reuses the same password across 4 different online services. If the probability that any single one of these services is successfully compromised via credential stuffing is 5%, what is the expected number of services compromised, using simple expected value (not compound probability)?

A 0.2

B 4

C 5

D 0.05

Question 60

A distributed denial-of-service (DDoS) attack takes a company's e-commerce website offline for 6 hours. The company estimates it generates an average of £45,000 in revenue per hour while the site is online. What is the estimated revenue lost due to the outage?

A £270,000
B £45,000
C £51,000
D £7,500

Answer key

1 D	**13** D	**25** B	**37** C	**49** D
2 C	**14** B	**26** B	**38** D	**50** A
3 C	**15** B	**27** C	**39** A	**51** B
4 D	**16** D	**28** D	**40** D	**52** C
5 A	**17** A	**29** B	**41** C	**53** D
6 A	**18** D	**30** B	**42** C	**54** B
7 D	**19** B	**31** A	**43** A	**55** D
8 D	**20** C	**32** C	**44** C	**56** B
9 C	**21** D	**33** D	**45** C	**57** B
10 A	**22** B	**34** B	**46** A	**58** B
11 C	**23** C	**35** C	**47** D	**59** A
12 B	**24** D	**36** C	**48** C	**60** A

Score: count your correct answers out of 60. Then work through the explanations below.

Answers and explanations

Question 1: D To provide a structured, documented record of identified risks, their assessed likelihood and impact, ownership, and the status of mitigating actions, supporting ongoing monitoring and accountability

A risk register provides a structured, documented record of an organisation's identified risks, capturing key information such as assessed likelihood and impact, the risk owner responsible for managing it, and the status of any mitigating actions — supporting ongoing monitoring, accountability, and periodic review as part of the broader ERM process, rather than being a static, one-off document. Describing it as purely a historical archive with no ongoing monitoring use misunderstands its core function as a live, regularly updated management tool. A risk register is one component within a broader ERM system that also requires board-level risk appetite setting and oversight — it does not replace the need for these other elements, which operate alongside and inform the risk register's content. Risk registers are meant to capture risks that could potentially occur, including those that have not yet materialised into an actual loss — restricting entries only to risks that have already caused financial harm would defeat much of the register's forward-looking, preventive purpose.

Section A, Risk registers as an enterprise risk management tool · Ref A1d · p3004

Question 2: C To provide generic guidelines and principles for effective risk management applicable across different types of organisation, rather than prescribing risk management activity specific to one industry or one particular type of risk

ISO 31000:2018 provides generic guidelines, principles, and a generic risk management process intended to be applicable and adaptable across many different types of organisation, industry sector, and risk category — it is explicitly designed as a flexible framework to be tailored to an organisation's specific context, rather than prescribing rigid, industry-specific or risk-specific activity. ISO 31000 is a voluntary international standard providing guidance, not a legally binding mandate imposed uniformly and without adaptation on every organisation regardless of context — organisations choose whether and how to adopt and adapt its principles. The standard is explicitly general in its intended application, not limited to financial services or any single sector — its principles and process are designed to be relevant across a wide range of organisational contexts. ISO 31000 does not itself define a specific, universal risk appetite for all organisations; risk appetite remains something each organisation must determine for itself based on its own specific circumstances, objectives and stakeholders, even while it may use ISO 31000's broader process guidance to help structure that determination.

Section A, ISO 31000 — risk management principles and process · Ref A1b · p3007

Question 3: C Effective ERM depends significantly on the tone set by governance and organisational culture, which shapes how the other framework components are actually put into practice

By positioning governance and culture as a foundational component within the five-component structure, COSO ERM 2017 signals that effective enterprise risk management is understood to depend significantly on the tone set by governance structures (board oversight, organisational structure, accountability mechanisms) and the underlying organisational culture (values, desired behaviours, understanding of risk) — these foundational elements shape how the other components (strategy and objective-setting, performance, review and revision, and information/communication/reporting) are actually implemented and lived out in practice, rather than governance and culture being a separate, disconnected consideration. Treating governance and culture as peripheral or optional ignores its explicitly foundational positioning within the framework and its demonstrated influence on how effectively the other components function in real organisations, as illustrated by scenarios where good formal processes are undermined by poor underlying culture. COSO ERM 2017 is designed to be broadly applicable across organisations of many types and sizes, not restricted to publicly listed companies specifically. Governance and culture within COSO ERM extends well beyond a narrow procedural matter such as board meeting frequency, encompassing broader dimensions including organisational values, accountability structures, attraction and development of capable individuals, and the way desired behaviours are reinforced across the organisation.

Section A, COSO ERM — the role of governance and culture as a foundational component · Ref A1b · p3015

Question 4: D Accept — since the cost of mitigation would exceed the expected impact, consciously retaining the risk without further action is the economically rational response

When the cost of mitigating a risk clearly exceeds its expected financial consequence, and the risk itself is low-probability and low-impact, Accept is the economically rational TARA response — the organisation consciously decides to retain the risk without further action, since spending more on mitigation than the risk is actually worth would itself be a poor use of resources. Avoidance (ceasing the underlying activity) would be a disproportionate response to a risk already assessed as low-probability and low-impact, and would forgo whatever benefit the activity itself provides. Transfer through insurance still incurs a premium cost, which for a genuinely low-impact risk may itself exceed the risk's expected consequence, making blanket insurance purchase for every risk regardless of cost an inefficient default rather than a sound universal rule. Reduce assumes some mitigation is always worthwhile regardless of cost-benefit — but the entire premise of this scenario is that mitigation cost exceeds expected benefit, which is precisely the condition under which Accept, not automatic reduction, is the more rational choice.

Section A, TARA framework — choosing between responses for a given risk · Ref A1a · p3016

Question 5: A Evaluating performance alongside the risk taken provides a fuller picture, since strong results from excessive risk may be less desirable than modest results within acceptable risk boundaries

COSO ERM's performance component emphasises evaluating actual results in relation to the risk taken to achieve them, since strong headline results achieved by taking on risk well beyond the organisation's stated appetite may be less sustainable, and arguably less genuinely successful, than more modest results achieved comfortably within acceptable risk boundaries — a manager who hits an aggressive target by taking excessive, unmanaged risk has not necessarily performed better than one who achieves a more modest but appropriately risk-managed result, even though the headline number alone might suggest otherwise. Treating performance and risk as entirely unrelated concepts contradicts this central premise of the framework's performance component, which explicitly links the two. Evaluating only the headline performance result while ignoring the risk taken to achieve it risks rewarding excessive risk-taking that may not be sustainable or aligned with the organisation's actual risk appetite — precisely the blind spot risk-adjusted performance evaluation is designed to address. This risk-adjusted view of performance is relevant across many types of organisation, not confined to financial services, even though risk-adjusted return concepts are also prominently used within that specific sector.

Section A, COSO ERM — the performance component and risk-adjusted performance · Ref A1b · p3017

Question 6: A Considering risk during objective-setting helps ensure objectives are realistic given the organisation's risk appetite, rather than discovering unacceptable risk only later

Considering risk as an integral part of objective-setting, rather than purely as a subsequent step, helps ensure the objectives themselves are realistic given the organisation's actual risk appetite and capacity — if risk is only considered after objectives are already fixed, the organisation may discover too late that the chosen objectives carry risk exposure well beyond what it is willing or able to bear, at a point where the objectives are already embedded in plans, budgets and stakeholder communications. This does not mean objectives become overly cautious — integrating risk consideration allows for informed, deliberate risk-taking in pursuit of ambitious objectives, rather than unrecognised risk being baked in by accident. Risk and objective-setting are explicitly and deliberately linked within COSO ERM's integrated approach, not treated as separate, unconnected processes. COSO ERM 2017's very title reflects this integration with strategy and objective-setting, directly contradicting a claim that it does not address objective-setting at all.

Section A, Enterprise risk management — linking risk to strategic objective-setting · Ref A1a · p3065

Question 7: D Review and revision recognises that risk exposures, the business environment, and organisational objectives all change over time, meaning the ERM framework itself needs periodic reassessment and adjustment to remain effective and relevant

COSO ERM includes review and revision as a distinct component because risk exposures, the broader business environment, and organisational objectives all change over time — an ERM framework designed to be effective under one set of circumstances may become progressively less well suited as those circumstances evolve, meaning periodic reassessment and adjustment of the framework itself is necessary to keep it genuinely effective and relevant, rather than assuming the initial design remains adequate indefinitely. This component is not concerned narrowly with mission statement wording — it addresses the effectiveness of the risk management framework and its components more broadly, evaluating whether they continue to function well as circumstances change. Treating an ERM framework as permanently complete and effective once designed ignores this well-recognised need for ongoing review, which the framework explicitly builds in as one of its five interrelated components rather than an optional afterthought. Review and revision is relevant to organisations of varying sizes and circumstances, not confined to very large organisations undertaking major transformation — even relatively stable organisations benefit from periodically confirming their ERM framework remains fit for purpose as smaller, incremental changes accumulate over time.

Section A, COSO ERM — the review and revision component · Ref A1b · p3068

Question 8: D The board's documented risk appetite should directly inform which option is more consistent with the risk it has stated it is willing to accept, not made in isolation from that

The board's documented risk appetite should directly inform which option is more consistent with the level and type of risk the organisation has stated it is willing to accept, ensuring the eventual strategic choice is not made in isolation from the organisation's own stated risk boundaries. Treating risk appetite as mainly a retrospective benchmark understates its intended role, which is forward-looking — to actively guide which options are consistent with the organisation's stated risk boundaries before a decision is made, not only to assess decisions after the fact. Always selecting the higher-return option regardless of documented risk appetite defeats the purpose of having a risk appetite statement at all, which exists specifically to constrain and inform choices between options with different risk-return profiles. Treating risk appetite as relevant only to operational decisions misses that board-level strategic choices are exactly the kind of decision a documented risk appetite is meant to inform, given their potential scale and impact on the organisation's overall risk profile.

Section A, Risk appetite — the relationship between risk appetite and strategic choice · Ref A1c · p3084

Question 9: C Incorporating upside risk means ERM also considers how the organisation can position itself to capture favourable, unexpected opportunities, not solely how to defend against and minimise adverse outcomes

Incorporating a broader view that recognises both downside threats and upside opportunities means ERM also considers how the organisation can position itself to recognise and capture favourable, unexpected developments — not solely how to defend against and minimise adverse outcomes — reflecting a more proactive, value-creating conception of risk management alongside its traditional defensive, loss-prevention role, consistent with COSO ERM 2017's broader integration with strategy and performance. Restricting ERM's scope exclusively to downside threats, treating any opportunity dimension as entirely outside its legitimate remit, reflects an older, narrower conception that more current ERM thinking has moved beyond. Downside risk (threats to be minimised) and upside risk (opportunities to be captured) are genuinely distinct concepts within this broader view, not interchangeable terms for the same thing — they call for different kinds of organisational response. Considering upside risk within ERM does not guarantee superior financial performance in every case — it provides a more complete framing of risk that can support better-informed decisions, but actual performance outcomes still depend on many other factors beyond simply how comprehensively risk is framed.

Section A, Enterprise risk management — upside risk and opportunity within ERM · Ref A1a · p3091

Question 10: A Effective board risk oversight can involve recognising genuine gaps in specialist knowledge and proactively supplementing it with external expertise, rather than assuming general experience is always sufficient

This practice illustrates that effective board risk oversight can involve honestly recognising genuine gaps in the board's own specialist knowledge — no board can reasonably be expected to have deep expertise in every specialist risk area, particularly fast-evolving ones such as advanced cyber threats — and proactively supplementing that gap with external expert input, rather than assuming general business experience and judgement, however substantial, is automatically sufficient for effectively overseeing every specialist risk area the organisation might face. Option B, claiming external expertise is always unnecessary if a board has general business experience overlooks the genuine value of deep, current, specialist knowledge that general business experience alone may not provide, particularly for fast-moving technical risk areas. Option C is wrong: seeking external expertise reflects thoughtful, proactive governance rather than an admission of fundamental inadequacy — recognising and addressing a specific knowledge gap is a sign of good governance practice, not evidence of a board being unfit for its broader role. Option D is wrong: supplementing board knowledge with external expertise is valuable whether or not a formal risk committee exists, and the whole board remains responsible for risk oversight.

Section A, Board oversight — using external risk expertise to supplement board knowledge · Ref A1e · p3121

Question 11: C An enterprise-wide view can reveal how a single underlying issue can create compounding, interconnected risk across multiple categories simultaneously, a connection that siloed, department-by-department risk management would likely miss by considering each risk category in isolation

This scenario illustrates the genuine value of an enterprise-wide, integrated view of risk — a single underlying issue (a delayed IT system upgrade) can create compounding, interconnected risk exposure across multiple distinct categories simultaneously (cyber, reputational, compliance), a connection that a siloed, department-by-department approach to risk management — where the IT department considers only IT-specific risk, compliance considers only compliance-specific risk, and so on, without cross-functional visibility — would likely miss entirely, since no single siloed function would necessarily see or be responsible for recognising the full combined picture across all affected categories. Claiming risk categories are always entirely independent with no possible connection directly contradicts this scenario's specific illustration of exactly such interconnection occurring in practice. A siloed approach is not inherently superior or more thorough — it can achieve depth within each specific specialist area, but at the cost of missing exactly this kind of important cross-category connection that only becomes visible when risk is considered holistically across the organisation, which is precisely the value ERM's integrated approach is designed to provide. This kind of interconnected risk pattern can arise in organisations of varying sizes and complexity, not confined to very large, complex organisations specifically — even smaller organisations can experience a single underlying issue creating compounding risk across multiple categories simultaneously.

Section A, Enterprise risk management — the interconnected nature of risks across an organisation · Ref A1a · p3135

Question 12: B A single audit opinion reflects conditions at a point in time and doesn't guarantee continued effectiveness afterward, so ongoing monitoring remains necessary since circumstances can change

A single positive internal audit opinion reflects the auditor's assessment of conditions and control effectiveness at a specific point in time — it does not guarantee that those same conditions and control effectiveness will continue indefinitely afterward, since circumstances can change (new staff, process changes, evolving risks) and control operation can deteriorate over time even after a genuinely positive assessment; ongoing monitoring, and periodic re-assessment through future audit cycles, remains necessary rather than treating a single past positive opinion as permanent, unconditional assurance requiring no further attention. Claiming a single opinion provides permanent, unconditional assurance ignores this basic point-in-time limitation applicable to any audit or assurance opinion. Internal audit opinions do provide genuine, valuable assurance when properly conducted — the limitation illustrated here is about the time-bound nature of any single assessment, not a claim that audit opinions have no value at all. This point-in-time limitation is not unique to internal audit — it applies equally to other forms of assurance, including external audit opinions, which similarly reflect conditions assessed at a specific point rather than providing permanent guarantees extending indefinitely into the future.

Section A, Assurance — limitations of relying on a single internal audit opinion · Ref A1f · p3138

Question 13: D Effective ERM depends on risk awareness and responsibility being genuinely shared across the organisation, not confined to a specialist risk department alone, since risks often first become visible to those closest to day-to-day operations, not to a centralised specialist function

Effective ERM depends on risk awareness and responsibility being genuinely shared across the organisation — consistent with the first-line ownership principle discussed within the three lines model — rather than confined to a specialist risk department alone, since risks (particularly operational and emerging risks) often first become visible to those closest to day-to-day operations, who may notice an emerging problem well before it would come to the attention of a centralised risk department with less direct visibility into daily operational detail. Believing a dedicated risk department alone is always fully capable of identifying and managing every risk without input from line managers and staff ignores this important first-line visibility advantage and risks exactly the kind of siloed 'not my responsibility' attitude the scenario describes. Risk management is not appropriately confined to board level alone either — the board provides oversight, but genuine risk management requires active engagement from operational management and staff throughout the organisation, not solely at the most senior governance level. Concentrating all risk responsibility in a single specialist department, rather than distributing genuine risk awareness and responsibility more broadly, does not reflect best practice — it reflects precisely the kind of responsibility gap and siloed thinking that undermines effective, organisation-wide risk management.

Section A, Enterprise risk management — risk management as a shared responsibility, not solely a specialist function · Ref A1a · p3144

Question 14: B 6

The tolerance threshold in monetary terms is calculated by applying the stated percentage to the relevant base figure (net assets): $200m x 0.03 = $6 million. Any risk with a potential loss above this threshold breaches the board's stated tolerance and requires specific escalation or mitigation. $3 million simply restates the tolerance percentage as if it were a dollar figure. $60 million would result from using 30% instead of the correct 3%, a misplaced decimal point. $200 million is simply the net assets figure itself, with no percentage applied at all.

Section A, Quantifying a risk tolerance threshold · Ref A1c · p3152

Question 15: B 1.5

A simple risk-adjusted performance ratio divides the return achieved by the level of risk taken to achieve it: 12% / 8% = 1.5. A higher ratio indicates more return generated per unit of risk taken, allowing comparison between divisions or strategies that achieved similar headline returns but with different levels of underlying risk. 0.7 would result from inverting the calculation (8%/12%) rather than dividing return by risk. 4.0 would result from incorrectly subtracting the risk from the return and treating the remainder as a ratio (12-8=4), rather than dividing. 96.0 would result from multiplying the two percentages together (12 x 8) rather than dividing one by the other.

Section A, Risk-adjusted performance ratio · Ref A1b · p3155

Question 16: D Business model obsolescence risk — particularly dangerous since reliable current profits can create a false sense of security, delaying adaptation until relevance has already eroded

This is business model obsolescence risk, which is particularly dangerous because a model that still generates reliable current profits can create a false sense of security, delaying necessary adaptation until the model's underlying relevance to customers and the market has already eroded significantly. Classifying it as financial risk misreads the scenario, which is about the strategic suitability of the business model itself, not a specific financial ratio or calculation. Treating a long record of reliable past profit as a strong predictor of continued future suitability is precisely the false sense of security the scenario warns against — clear signals that customer needs and the competitive landscape are shifting are described as already present, regardless of current profitability. Classifying it as cyber risk misreads the scenario, which describes a broader failure to adapt the business model to shifting customer needs and competition, not a threat originating from a digital or information security source.

Section B, Strategic risk — risk from failure to adapt the business model · Ref B1c · p3020

Question 17: A Strategic risk can arise when a key assumption underlying the strategy is invalidated by real-world events, highlighting the need to periodically test such assumptions

This scenario illustrates that strategic risk can arise specifically when a key underlying assumption on which the strategy was originally built — here, an assumption of continuing political and economic stability in a key trading partner's jurisdiction — becomes invalidated by subsequent real-world events, highlighting why periodically identifying and stress-testing the key assumptions embedded in a strategy is an important, ongoing part of strategic risk management, rather than treating those assumptions as permanently fixed once the strategy has been initially developed and approved. Describing political and economic developments in another jurisdiction as entirely outside the scope of an organisation's strategic risk considerations ignores how directly such external developments can affect supply chains, market access and overall strategic viability, as the scenario explicitly demonstrates. Strategic assumptions genuinely do warrant periodic revisiting throughout a strategy's life, particularly where the external environment they depend on can plausibly change — assuming a fixed, permanent status for assumptions is precisely the practice that leaves organisations exposed to exactly this kind of risk. This type of disruption from external political and economic instability can affect organisations of many different sizes with international exposure, including large, well-resourced multinationals, not merely small organisations with limited resources.

Section B, Strategic risk — assumptions underpinning strategy becoming invalidated · Ref B1a · p3021

Question 18: D Partner alignment risk within strategic alliances — thorough due diligence on a prospective partner's genuine long-term strategic interests and objectives before committing to an alliance can help identify potential misalignment earlier

This is partner alignment risk within strategic alliances; thorough due diligence on a prospective partner's genuine long-term strategic interests and objectives before committing to an alliance can help identify potential misalignment earlier, before it undermines the alliance's objectives. A signed formal agreement addresses process and governance, but does not itself guarantee that the partners' underlying strategic interests remain aligned over time — the scenario describes exactly this kind of divergence emerging despite the alliance having been formally agreed. Classifying it as purely operational risk understates the issue: the friction described stems from a genuine divergence in the partners' own long-term strategic direction, not simply a day-to-day execution problem. Classifying it as purely reputational risk also understates the issue, since the described friction is undermining the alliance's actual strategic objectives, not merely how the situation might look to outside observers.

Section B, Strategic risk — risk arising from strategic partnerships and alliances · Ref B1a · p3024

Question 19: B Technology obsolescence risk — challenging to monitor because the pace and success of an emerging alternative technology are genuinely uncertain, making timing hard to predict

This scenario illustrates technology obsolescence risk — the risk that a company's core underlying technology becomes outdated and commercially non-viable as an alternative technology improves and gains adoption. Monitoring this risk can be particularly challenging because the pace of improvement, eventual commercial success, and adoption timeline of an emerging alternative technology are often genuinely uncertain at an early stage — many emerging technologies fail to achieve widespread adoption or take far longer than initially expected, while others progress and displace incumbents faster than anticipated, making the specific timing and even the ultimate likelihood of obsolescence difficult to predict with real confidence, complicating decisions about when and how much to invest in response. The claim that an established, successful core technology can never become obsolete under any future circumstances contradicts extensive well-documented historical examples of exactly this kind of technology displacement occurring across many industries. This is a broader strategic risk concerning the company's core product viability, not confined to a narrow cybersecurity or information-security framing, and its analysis requires genuine strategic and technological judgement, extending well beyond narrow financial statement metrics alone.

Section B, Strategic risk — technology obsolescence risk to core products or services · Ref B1c · p3026

Question 20: C The risk of misjudging a genuine, sustained shift in customer preferences, continuing to invest in declining demand rather than reallocating towards growing interest

This scenario illustrates the risk of misjudging or failing to adequately respond to a genuine, sustained shift in customer preferences — continuing to invest heavily in expanding capacity for a product category with steadily declining underlying demand, rather than recognising the trend and reallocating resources towards areas of genuine and growing customer interest, represents a strategic misjudgement that can result in significant capital being committed to an area of diminishing rather than growing value. Describing continued investment in an existing category as always objectively correct, regardless of subsequent evidence about declining demand, ignores the entire premise of strategic risk monitoring, which exists precisely to detect and respond to this kind of evolving evidence rather than persisting with a fixed prior assumption regardless of new information. This scenario has no inherent cybersecurity dimension — it concerns strategic judgement about market demand trends, not information security. Changing customer preferences can arise from many different underlying drivers — social trends, technological alternatives, changing values, demographic shifts — not solely or even primarily from new government regulation, making the regulatory-risk framing an inaccurate characterisation of this particular scenario.

Section B, Strategic risk — risk from misjudging changing customer preferences · Ref B1a · p3027

Question 21: D Key person dependency risk — succession planning and deliberate knowledge transfer processes can help reduce the organisation's vulnerability to the sudden loss of these critical individuals

This scenario illustrates key person dependency risk — significant reliance on a small number of individuals whose expertise and relationships underpin competitive position creates real vulnerability if any of them were to leave, become incapacitated, or otherwise become unavailable, particularly where no documented succession plan or deliberate knowledge transfer process exists to preserve institutional knowledge and relationships. Succession planning (identifying and developing potential successors in advance) and deliberate knowledge transfer processes (documenting critical knowledge and actively transferring relationships and expertise to others within the organisation) are widely recognised practices that can help reduce this vulnerability over time. Describing heavy reliance on a small number of key individuals as inherently the safest organisational structure, with no qualification, ignores the genuine concentration risk this creates, which the absence of succession planning specifically compounds. This is a broader talent and organisational risk, not a cybersecurity matter, and its analysis requires understanding of organisational capability and relationships, extending well beyond narrow financial statement metrics.

Section B, Strategic risk — talent and key person dependency risk · Ref B1c · p3028

Question 22: B ESG-related strategic risk — failing to integrate environmental considerations into strategic planning can expose the company to investor pressure, shifting customer preferences, and regulatory consequences

This scenario illustrates ESG-related strategic risk — failing to integrate environmental (and more broadly, social and governance) considerations into core strategic planning can expose the company to multiple converging pressures: investors increasingly factoring ESG performance into capital allocation decisions, customers shifting preferences towards more sustainable providers, and regulators introducing more stringent environmental requirements — each of which is becoming an increasingly significant strategic factor across many industries, not a peripheral compliance afterthought. Describing environmental considerations as entirely irrelevant to strategic planning ignores this well-documented and growing significance across investor, customer and regulatory dimensions, which the scenario explicitly describes as already exerting pressure on this company. This is not a cybersecurity risk — ESG risk concerns environmental, social and governance factors, a genuinely distinct risk category from information security. ESG-related strategic risk extends well beyond narrow financial statement metrics, encompassing broader stakeholder relationships, regulatory positioning, and long-term strategic resilience considerations that financial statements alone would not fully capture.

Section B, Strategic risk — environmental, social and governance (ESG) risk · Ref B1b · p3030

Question 23: C Macroeconomic risk arising from an inflexible plan built on a single set of economic assumptions — incorporating scenario analysis or contingency planning for alternative macroeconomic conditions can help build greater strategic resilience

This scenario illustrates macroeconomic risk arising from a strategic plan built rigidly around a single set of economic assumptions (continued low interest rates and stable inflation) with no contingency for alternative conditions — if those assumptions prove wrong, as macroeconomic conditions are genuinely prone to changing over a multi-year strategic horizon, the plan's underlying economics (financing costs, cost base, customer purchasing power) could be significantly disrupted, with no pre-considered response ready. Incorporating scenario analysis (testing the strategy against several plausible macroeconomic futures) or explicit contingency planning (pre-agreed adjustments if conditions shift materially) can help build greater strategic resilience against this kind of macroeconomic uncertainty, rather than leaving the organisation exposed to a single fixed assumption set. Describing interest rates and inflation as permanently stable over any multi-year period contradicts well-documented historical experience of meaningful macroeconomic fluctuation over such timeframes. This is not a cybersecurity risk, and while reputational consequences could conceivably follow from a poorly managed macroeconomic shock, the risk itself concerns the plan's underlying financial and operational viability, not primarily external public image.

Section B, Strategic risk — macroeconomic risk and its strategic implications · Ref B1c · p3031

Question 24: D The organisation risks being caught unprepared by emerging strategic threats or opportunities that a more deliberate, formal horizon-scanning process might have identified at an earlier, more addressable stage

Focusing strategic monitoring almost exclusively on well-established, currently visible competitors and trends risks the organisation being caught unprepared by emerging strategic threats or opportunities that were, at an earlier stage, only weak or distant signals — a more deliberate, formal horizon-scanning process, actively looking beyond the current, obvious competitive landscape for weaker signals of change (in technology, customer behaviour, regulation, or broader societal trends), can identify potentially significant developments earlier, while there is still more time and more options available to respond effectively, rather than only recognising the threat once it has already become an established, currently visible competitor or trend. Claiming exclusive focus on currently visible factors is always fully sufficient ignores the well-documented pattern of significant strategic disruptions that were, in their earlier stages, exactly the kind of weak, easily dismissed signal that a narrow monitoring approach would miss entirely. Horizon scanning has a demonstrated track record of surfacing strategically significant trends across many industries at an early stage — describing it as completely worthless contradicts this established value. Horizon scanning is a practice relevant to organisations of varying sizes engaged in strategic planning, not confined to very large multinationals specifically, even though larger organisations may have more dedicated resource to conduct it more formally.

Section B, Strategic risk — risk from inadequate horizon scanning of emerging trends · Ref B1a · p3032

Question 25: B Single point of failure risk — a significant disruption to that one facility (fire, natural disaster, equipment failure) could halt the entire product line's output; developing alternative or backup production capability can help reduce this concentrated vulnerability

Relying on a single production facility for an entire critical product line's output represents a single point of failure — a significant disruption to that one facility, whether from fire, natural disaster, equipment failure, or other cause, could halt the entire product line's output with no alternative source of supply, creating concentrated vulnerability that a more distributed production approach would not carry to the same degree. Developing alternative or backup production capability — whether through a second facility, contracted third-party capacity, or other means — can help reduce this concentrated vulnerability, even though doing so typically involves additional cost that must be weighed against the risk being addressed. Describing single-facility reliance as always the most efficient, lowest-risk approach ignores the genuine concentration risk this creates — efficiency gains from a single facility must be weighed against the loss of resilience that distributed capability would provide. This is a broader strategic and operational risk concerning production resilience, not a cybersecurity matter specifically. Single point of failure risk in critical production or infrastructure can affect organisations of varying sizes and capital bases, including large, well-capitalised organisations — capital availability does not by itself eliminate the underlying concentration risk if production remains centralised in a single facility.

Section B, Strategic risk — single point of failure in critical infrastructure or processes · Ref B1c · p3086

Question 26: B The risk that genuine strategic drift is mislabelled as intentional adaptation, masking the fact that no real strategic reassessment has occurred and potentially delaying the kind of genuine review that would catch a real problem

This illustrates the risk that genuine strategic drift is mislabelled as intentional adaptation, masking the fact that no real strategic reassessment has occurred and potentially delaying the kind of genuine review that would catch a real problem. Treating management's own confidence in the 'deliberate adaptive flexibility' label as a reliable indicator of genuine reassessment is exactly the assumption the scenario shows to be false — the label is applied despite no real strategic reassessment having actually taken place. Treating this purely as a communications or reporting matter understates the risk, since the substantive problem is the absence of any genuine strategic review, not merely how the situation is described or reported. There is no basis in the scenario for assuming this mischaracterisation is more likely in organisations with formal, well-documented planning processes; if anything, weaker or less rigorous planning discipline, not extensive documentation, is the more plausible setting for genuine drift to go unreviewed.

Section B, Strategic risk — risk arising from strategic drift being mistaken for deliberate adaptation · Ref B1c · p3094

Question 27: C Demographic concentration risk — reliance on a shrinking segment without a strategy for growing segments risks a gradually eroding customer base as the population structure shifts

This scenario illustrates demographic concentration risk — reliance on a customer base concentrated in a demographic segment that is shrinking as a proportion of the overall population, without any strategic effort to also appeal to growing younger segments, risks a gradually eroding customer base over time as the underlying population structure continues to shift in ways the company's current strategy is not positioned to capture. Claiming demographic trends have no bearing on an individual company's customer base or strategic position ignores how directly population structure shifts can affect long-term demand for products and services particularly associated with specific age groups. This is not a cybersecurity risk — demographic and societal trend risk concerns broader population and market structure shifts, a genuinely distinct risk category from information security. Demographic concentration risk can affect companies across many industries whose customer base or workforce is concentrated in a particular demographic segment, not confined to the retail sector specifically — sectors ranging from financial services to healthcare to media can face analogous demographic-related strategic risk.

Section B, Strategic risk — demographic and societal trend risk · Ref B1a · p3095

Question 28: D The risk of inadequate crisis response capability — without prior planning, an organisation facing a major crisis is likely to respond more slowly and less effectively than one that prepared in advance

This scenario illustrates the risk of inadequate crisis response capability — without prior planning, established protocols, and a trained response team, an organisation facing a genuine major crisis (whatever its specific nature — reputational, operational, safety-related, or otherwise) is likely to respond more slowly, less coherently, and potentially less effectively than one that has invested in advance crisis management preparation, precisely because the difficult coordination and decision-making work has not been done in advance, leaving the organisation to work out its approach for the first time under the pressure and confusion a genuine crisis typically brings. Assuming a major crisis is unlikely enough that dedicated preparation is never worthwhile underestimates both the range of events that could constitute a genuine crisis and the potentially severe consequences of an inadequate response if one does occur — many organisations that assumed this way have subsequently faced exactly the kind of poorly coordinated crisis response this lack of preparation predicts. This is not a cybersecurity risk specifically — while a cyber incident could be one type of trigger for a crisis, crisis management capability as a broader strategic risk concern extends well beyond cyber-specific triggers to any type of major crisis event. Crisis management preparedness is a relevant consideration for organisations of varying sizes and industries, not confined to very large organisations in high-risk industries specifically — smaller organisations and those in seemingly lower-risk industries can and do face significant crises requiring an effective, prepared response.

Section B, Strategic risk — risk from an inadequate crisis management capability · Ref B1b · p3104

Question 29: B Innovation underinvestment risk — persistently under-investing relative to competitors risks a gradual erosion of competitive position as rivals develop superior products the company can't match

This scenario illustrates innovation underinvestment risk — persistently investing less in research and innovation than main competitors, in favour of short-term margin preservation, risks a gradual erosion of competitive position over the longer term as rivals develop superior products, services, processes or capabilities that the company's more limited innovation investment increasingly struggles to match, potentially leaving the company competitively disadvantaged even though its short-term margins may have looked comparatively stronger during the period of underinvestment. Claiming short-term margin preservation over innovation investment is always the objectively correct choice, regardless of competitors' relative investment levels, ignores this genuine longer-term competitive erosion risk that sustained underinvestment relative to more innovation-active rivals can create. This is not a cybersecurity risk — innovation investment strategy concerns competitive positioning and capital allocation, an entirely distinct risk category from information security. While the pace of required innovation investment can be particularly intense in fast-moving technology sectors, the underlying risk of competitive erosion from sustained relative innovation underinvestment can affect companies across many industries, including more traditional or slower-moving ones, wherever competitors are meaningfully out-investing in improving their offering over time.

Section B, Strategic risk — risk from underinvestment in innovation relative to competitors · Ref B1c · p3146

Question 30: B £2,600,000

Expected value combines each possible outcome weighted by its probability: (0.60 x £5,000,000) + (0.40 x -£1,000,000) = £3,000,000 - £400,000 = £2,600,000. A positive expected value suggests the decision is worthwhile on average, though the board would also need to weigh the risk of the 40% downside scenario against its risk appetite, not rely on expected value alone. £3,000,000 only reflects the weighted upside scenario and omits the weighted downside loss entirely. £3,400,000 would result from adding rather than subtracting the weighted loss (£3,000,000 + £400,000). £4,000,000 simply combines the two raw outcomes (£5,000,000 − £1,000,000) without weighting either by its probability.

Section B, Expected value of a strategic decision · Ref B1a · p3156

Question 31: A Inherent risk = susceptibility before controls; control risk = controls fail to catch it; detection risk = review also fails — all three combine

These three risk concepts combine to describe the overall risk that a material error or issue goes unaddressed. Inherent risk is the susceptibility of an area to error or issue arising in the first place, before considering the effect of any internal controls — some areas are inherently more prone to error due to their complexity, judgement involved, or susceptibility to manipulation. Control risk is the risk that the organisation's internal controls fail to prevent or detect such an error, even though controls exist and are intended to catch it. Detection risk is the risk that additional review, audit or other verification procedures also fail to catch the error even after both inherent susceptibility and any control gaps have already allowed it through. Together, these three combine (conceptually multiplicatively, in formal audit risk model terms) to determine the overall risk of an issue going unaddressed — reducing any one of the three (for example, strengthening controls to reduce control risk) reduces the overall combined risk. Treating the three as interchangeable, or asserting only one is ever relevant, ignores this well-established and examinable three-part structure, and the roles are also reversed in the third option relative to their standard definitions.

Section C, Inherent risk, control risk and detection risk distinguished · Ref C1b · p3037

Question 32: C A compliance audit — assessing adherence to specific external regulatory or internal policy requirements, distinct from a value-for-money audit or a fraud audit

A review specifically assessing adherence to a defined set of external regulatory requirements (or, similarly, internal policies) is a compliance audit — a distinct type of internal audit engagement from a value-for-money audit, which more broadly assesses the economy, efficiency and effectiveness of how resources are used (regardless of specific regulatory compliance), or a fraud audit, which specifically investigates suspected or potential fraudulent activity, typically triggered by a specific concern or red flag rather than a routine regulatory compliance check. Internal audit functions typically conduct several genuinely distinct types of engagement — including compliance audits, value-for-money audits, fraud audits, and social/environmental audits, among others — each with a different specific focus and objective, rather than performing an identical, undifferentiated type of review in every engagement. Compliance with regulatory requirements and investigation of suspected fraud are genuinely distinct concerns with different triggers, methods and objectives, even though a compliance audit could incidentally uncover indicators warranting a separate fraud investigation.

Section C, Internal audit — types of internal audit engagement · Ref C1d · p3039

Question 33: D Reporting to an independent level helps preserve the internal audit function's objectivity, reducing the risk that findings are influenced or suppressed by the very management whose performance and controls are being assessed

Reporting administratively and functionally to a level independent of the specific operations being audited — typically the audit committee or a similarly independent governance body — helps preserve internal audit's objectivity, since a function that instead reported directly to, and had its performance evaluated by, the very manager whose department it is assessing would face an obvious and significant conflict of interest, with a real risk that unfavourable findings are softened, delayed, or suppressed to avoid displeasing the person controlling the auditor's own position and evaluation. Claiming reporting line has no bearing on objectivity ignores this well-established governance rationale, which is precisely why independent reporting lines for internal audit are a standard feature of good governance frameworks. Reporting internal audit findings directly to the audited manager, rather than to an independent body, would create exactly the conflict of interest this independence requirement is designed to prevent, making it a poor rather than optimal reporting arrangement. Internal audit independence is a relevant and important governance consideration for organisations of varying sizes that maintain an internal audit function, not confined to very large multinationals specifically.

Section C, Internal audit — independence and objectivity requirements · Ref C1e · p3040

Question 34: B Senior leadership's demonstrated commitment to integrity significantly influences how seriously controls are taken elsewhere, since employees take cues from observed behaviour, not just stated policy

'Tone at the top' refers to senior leadership's demonstrated commitment — through actual behaviour, not merely stated policy — to integrity, ethical values and taking internal control seriously; this matters significantly because employees throughout the organisation often take genuine cues about what actually matters from observed leadership behaviour rather than from written policy alone, meaning that if senior leaders are seen to bypass controls or treat compliance as a mere formality, this behavioural signal can undermine control effectiveness throughout the organisation far more than any written policy statement could offset. The term has no connection to font or visual formatting choices in policy documents — it refers to substantive leadership behaviour and demonstrated values, not document styling. Senior leadership behaviour has a well-documented and significant influence on organisational culture and control-following behaviour throughout an organisation — describing it as having no meaningful influence contradicts this well-established governance and behavioural principle. Tone at the top is relevant to internal control effectiveness on an ongoing, year-round basis, not confined to how leadership behaves specifically during an annual external audit visit.

Section C, Control environment — tone at the top · Ref C1a · p3042

Question 35: C Economy (acquiring resources at appropriate cost and quality), efficiency (converting inputs to outputs with minimal waste), and effectiveness (achieving intended outcomes and objectives)

Value-for-money audits are typically structured around three related dimensions, often called 'the three Es': economy (whether resources of appropriate quality are acquired at appropriate cost), efficiency (whether inputs are converted into outputs with minimal waste, maximising output for a given level of input or minimising input for a given level of output), and effectiveness (whether the outputs actually achieve the intended outcomes and objectives the resources were deployed to pursue). This is a distinct framing from a narrow revenue/cost/profit financial statement analysis — VFM audit specifically examines resource use in relation to economy, efficiency and effectiveness, which is a broader and more specifically operational lens than pure financial statement metrics. Compliance, fraud and cybersecurity are each separate, distinct types of audit engagement with their own specific focus, not the defining dimensions of a value-for-money audit specifically. Governance, culture and reputation are relevant broader organisational considerations but are not the specific three dimensions that define the scope of a value-for-money audit, which centres on economy, efficiency and effectiveness of resource use.

Section C, Internal audit — value-for-money audits and the three Es · Ref C1d · p3043

Question 36: C A risk-based approach, prioritising audit coverage towards the areas assessed as carrying the greatest risk to the organisation's objectives, making the most effective use of limited audit resources

A risk-based approach to internal audit planning — prioritising audit coverage towards the areas assessed as carrying the greatest risk to the organisation's objectives — is generally considered best practice, since it makes the most effective use of inevitably limited audit resources by concentrating audit effort where it is likely to add the most value and provide assurance over the areas that matter most, rather than spreading effort evenly or arbitrarily across all areas regardless of their actual relative significance. An alphabetical rotation approach ignores actual risk levels entirely, potentially leaving genuinely high-risk areas under-audited for extended periods purely because of where their name falls in an arbitrary ordering. Auditing only areas senior management personally prefers, without independent risk-based prioritisation, risks internal audit's independence and objectivity being compromised, and may systematically miss genuinely high-risk areas that management would prefer not to have scrutinised. Refusing to ever revisit a previously audited area, regardless of its current assessed risk level, ignores that risk levels change over time — an area assessed as lower risk in the past may become significantly higher risk later, warranting renewed audit attention under a genuinely risk-based approach.

Section C, Internal audit — planning and risk-based audit prioritisation · Ref C1d · p3047

Question 37: C Without a formal follow-up process, there is a risk that identified control weaknesses remain unaddressed despite being identified, undermining the practical value of the audit work performed, since identification alone does not itself fix the underlying weakness

Without a formal process for tracking whether management has actually implemented recommendations following identified control weaknesses, there is a real risk that those weaknesses remain unaddressed indefinitely despite having been identified and formally reported, since identification and reporting alone do not themselves fix the underlying weakness — implementation still depends on management taking the recommended action, and without follow-up, there is no mechanism confirming whether this has actually happened, undermining much of the practical value the original audit work was intended to deliver. Assuming identification and reporting automatically results in implementation ignores the genuine possibility of management inaction, competing priorities, or simple oversight, which is precisely why follow-up tracking is considered an important element of a complete audit cycle rather than a redundant additional step. While the initial identification and reporting represents a discrete piece of audit work, many internal audit functions consider tracking recommendation implementation as a legitimate and valuable extension of their role, closing the loop on the audit process — this is not considered inherently outside internal audit's proper scope. Tracking recommendation implementation is commonly performed by internal audit itself (sometimes alongside audit committee oversight of the tracking), rather than being a task exclusively assigned to external audit, whose engagement scope and objectives are generally different from ongoing internal recommendation tracking.

Section C, Internal audit — reporting findings and follow-up on recommendations · Ref C1d · p3051

Question 38: D Inherent limitations include human error, collusion, management override, and cost-benefit design trade-offs

Internal control frameworks explicitly recognise several inherent limitations that mean even a well-designed and properly operating system cannot provide absolute assurance: the possibility of human error or flawed judgement in performing controls; the potential for collusion between two or more individuals to override segregation of duties designed to require independent action by separate people; the risk of management override, where senior individuals with sufficient authority bypass controls that would otherwise apply; and the practical reality that controls are typically designed weighing their cost against the benefit of risk reduction they provide, meaning some residual risk is knowingly accepted rather than designing controls against every conceivable scenario regardless of cost. Claiming a sufficiently well-designed system can provide complete, absolute assurance contradicts this well-established recognition of inherent limitations within control frameworks and audit standards more broadly — 'reasonable', not absolute, assurance is the standard typically referenced. Inadequate training is one potential contributing factor to control failure, but it is not the only inherent limitation — collusion, management override and cost-benefit design boundaries are equally recognised and distinct limitations. These inherent limitations apply to organisations of all sizes, including large, well-resourced organisations with sophisticated control systems — sophistication reduces but does not eliminate the fundamental limitations described, which is why even the most well-resourced organisations still experience occasional control failures and fraud.

Section C, Limitations of internal control — inherent limitations that no system can fully eliminate · Ref C1b · p3052

Question 39: A Ongoing evaluations give real-time visibility; separate evaluations give periodic independent depth — using both is complementary

Ongoing evaluations are built into normal, day-to-day business processes and management activities, providing real-time or near-real-time information about whether controls are functioning as intended, often through routine supervisory review or automated system checks. Separate evaluations are conducted periodically, often by a party more independent of daily operations (such as internal audit), providing a more independent and typically more in-depth assessment at scheduled intervals. Using both provides complementary monitoring coverage: ongoing evaluations offer more immediate, continuous visibility, while separate evaluations offer periodic, more independent and thorough assessment, catching issues that day-to-day ongoing monitoring alone might miss due to its more embedded, potentially less independent nature. The terminology is reversed in the third option relative to its standard COSO usage. Using both types together is a recognised and generally recommended approach for comprehensive monitoring, rather than being inherently duplicative — each serves a genuinely different, complementary purpose within the overall monitoring component.

Section C, COSO — monitoring activities: ongoing versus separate evaluations · Ref C1a · p3073

Question 40: D It ensures decisions of a given significance get appropriately senior scrutiny; if not followed, decisions may be approved at too junior a level, undermining oversight

A delegated authority matrix serves the control purpose of ensuring that decisions or transactions of a given significance (as measured by value or other criteria) receive an appropriately senior level of scrutiny and approval before proceeding, reflecting the principle that more significant decisions warrant more senior oversight. If the matrix is not consistently followed in practice — for example, a transaction requiring senior management approval is instead approved at a junior level — the intended level of oversight for significant transactions is undermined, potentially allowing decisions to proceed without the scrutiny the organisation intended to require for matters of that significance. Option A, describing the matrix as a purely administrative formality with no bearing on actual oversight ignores its substantive control function in ensuring proportionate scrutiny is genuinely applied. Option B is wrong: departures from a documented authority matrix could arise from various causes — including simple oversight, inadequate training or communication of the requirements, or in some cases inappropriate circumvention — not exclusively deliberate fraud in every instance, though investigation of departures remains important regardless of cause. Option C is wrong: a delegated authority matrix is a standing control over who may approve what, and it applies whether or not board members agree with one another.

Section C, Control activities — approval limits and delegated authority matrices · Ref C1c · p3076

Question 41: C Weaknesses can affect operations and compliance too, not just financial reporting — a narrow focus would miss these risks

Internal control weaknesses can genuinely affect operational efficiency (such as wasted resources from poor process controls) and compliance with applicable laws and regulations (such as failing to meet a specific regulatory requirement due to inadequate compliance monitoring), not solely the accuracy of financial reporting — a control framework focused narrowly on financial reporting objectives alone would miss significant risks to these other important categories of organisational objective, which is precisely why COSO's framework explicitly addresses operations and compliance alongside reporting, reflecting a genuinely comprehensive view of what internal control is meant to support achieving. Claiming COSO's framework is concerned exclusively with financial reporting, with operations and compliance entirely outside its scope, misrepresents the framework's actual, explicitly broader three-category structure. Achieving financial reporting objectives does not automatically guarantee that operational efficiency or regulatory compliance objectives are also being met — these are genuinely distinct categories of objective that can each be undermined by different specific control weaknesses, requiring separate consideration rather than assuming one guarantees the others. Internal control relevance to operational and compliance objectives extends across organisations in many different sectors, not confined to heavily regulated industries specifically — even less heavily regulated organisations have operational efficiency and applicable legal compliance objectives that internal control can support or undermine.

Section C, COSO — the relevance of internal control across all types of organisational objectives · Ref C1a · p3119

Question 42: C Inadequate oversight of outsourced processes — outsourcing doesn't eliminate the organisation's own responsibility for ensuring adequate control exists, so ongoing monitoring or periodic independent assurance remains important

This scenario illustrates inadequate oversight of outsourced processes — outsourcing a process such as payroll to a third-party provider does not eliminate the outsourcing organisation's own underlying responsibility for ensuring adequate control exists over that process, since errors, fraud, or control failures at the third-party provider can still directly affect the outsourcing organisation and its stakeholders (employees relying on accurate, timely payroll, for example); ongoing monitoring or periodic independent assurance over the outsourced arrangement — such as reviewing the third-party provider's own independent audit reports covering its control environment (sometimes called a service organisation control report), or conducting the organisation's own periodic review — remains an important control activity rather than something outsourcing itself can substitute for. Option A, claiming outsourcing automatically and fully transfers control responsibility away from the outsourcing organisation misunderstands this continuing underlying responsibility, which many regulatory and governance frameworks explicitly recognise cannot simply be outsourced away along with the operational task itself. Option B is wrong: assuming a third party's processes are adequately controlled without any verification is not an efficient control approach — it is an unverified assumption that leaves the outsourcing organisation exposed to control failures at the provider it has no visibility into. Option D is wrong: the need for oversight does not depend on where the provider is located, since a domestic provider's control failures affect the organisation just as much.

Section C, Control activities — controls over outsourced or third-party managed processes · Ref C1c · p3123

Question 43: A Technically accurate findings provide limited value if not communicated clearly enough for the audience to act on, so effective reporting needs clear, accessible communication, not accuracy alone

Technically accurate findings provide limited practical value if they are communicated in a way the intended audience — senior management and the audit committee, who are not necessarily technical specialists in the specific area audited — cannot readily understand and translate into clear, prioritised action, since the whole point of audit reporting is to drive appropriate management response and, where needed, governance-level attention to significant issues; effective audit reporting therefore requires clear, accessible communication genuinely tailored to its intended audience, alongside technical accuracy, not technical accuracy in isolation from how well the findings are actually communicated and understood. Claiming technical accuracy is the only factor that matters, regardless of communication clarity, ignores this practical reality that a technically correct finding delivers no value if its intended recipients cannot readily understand and act on it. Deliberately maximising technical density, treating accessibility as an inappropriate compromise of rigor, misunderstands that clear communication and technical rigor are not in genuine tension — accurate findings can and should be presented clearly for a non-specialist audience without sacrificing their underlying technical accuracy. Communication clarity matters for audit reports directed at any level of the intended audience, not solely very senior audiences such as the full board — operational management audiences equally benefit from, and require, clear, actionable reporting rather than unnecessarily dense technical language.

Section C, Internal audit — communicating audit results in a way that drives action · Ref C1d · p3133

Question 44: C £25,000

The control reduces the expected loss from £60,000 to £15,000, a reduction of £45,000. Deducting the £20,000 annual cost of operating the control gives a net annual benefit of £25,000, meaning the control is cost-justified on a straightforward expected-value basis. £45,000 is only the reduction in expected loss, without deducting the cost of the control itself. £20,000 simply restates the cost of the control on its own, not the net benefit after accounting for the loss reduction it achieves. £60,000 is simply the original expected loss without the control, not the net benefit of implementing it.

Section C, Cost-benefit analysis of a proposed control · Ref C1c · p3161

Question 45: C £160,000

The materiality threshold is calculated by applying the chosen percentage to the relevant base figure: £8,000,000 x 0.02 = £160,000. Items or errors below this threshold would generally not be considered significant enough on their own to warrant escalation, whereas items above it would require further investigation or disclosure. £80,000 would result from using 1% instead of the correct 2%. £16,000 would result from using 0.2% instead of the correct 2%, a misplaced decimal point. £800,000 would result from using 10% instead of the correct 2%.

Section C, Setting a materiality threshold · Ref C1c · p3162

Question 46: A Ransomware — it primarily targets the availability of data and systems, denying the organisation access to its own information until a ransom demand is met (or the data is otherwise recovered)

This scenario describes ransomware — malicious software that encrypts an organisation's files, rendering them inaccessible, and then demands payment (typically in cryptocurrency) in exchange for the decryption key needed to restore access. Ransomware primarily targets the availability of data and systems — the organisation typically still has its data, but cannot access or use it without the decryption key, distinguishing this from attacks that instead target confidentiality (unauthorised viewing of data) or integrity (unauthorised alteration of data). A virus is a genuinely distinct category of malware — self-replicating code that attaches to legitimate programs — which, while it can sometimes be used to deliver ransomware, is not definitionally identical to ransomware itself. Spyware covertly monitors and collects information about user activity without their knowledge, a fundamentally different mechanism and objective from encrypting files and demanding payment. Ransomware is a category of malicious software, not a firewall configuration vulnerability — firewalls are a defensive control that can help prevent malware delivery, not the malware itself.

Section D, Cyber risk — malware categories and mechanisms · Ref D1a · p3053

Question 47: D It provides a framework and set of requirements for establishing, implementing, maintaining and continually improving an information security management system, covering people, processes and technology, not solely technical controls

ISO 27001 provides an internationally recognised framework and set of requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) — deliberately covering people (roles, training, awareness), processes (policies, procedures, risk assessment) and technology (technical controls) together, rather than being a narrow, purely technical specification, reflecting the reality that effective information security depends on more than technology alone. It is not a hardware configuration specification for firewalls specifically — it addresses information security management holistically, including but not limited to specific technical control choices, which individual organisations determine based on their own risk assessment within the ISO 27001 framework's broader structure. The standard is applicable to organisations across both public and private sectors internationally, not restricted to government bodies alone. ISO 27001 does not mandate use of a single, identical, prescribed software product across all certified organisations — it sets out a risk-based management system framework within which organisations select and implement controls appropriate to their own specific risk assessment and context, allowing for considerable variation in the specific technical and procedural choices made by different certified organisations.

Section D, Cyber risk — ISO 27001 information security management · Ref D1c · p3056

Question 48: C The delay leaves a known, publicly disclosed vulnerability unaddressed, creating a window attackers could exploit; timely patch management closes this window as quickly as practical

Delaying a security patch for a known, publicly disclosed vulnerability leaves that vulnerability unaddressed for longer than necessary, creating a window of exposure that attackers can exploit — attackers often specifically monitor for and target known, publicly disclosed vulnerabilities in organisations that have not yet applied the available fix. Timely patch management — applying available security patches as promptly as practical, balanced against genuine operational considerations — closes this window of known exposure before it can be exploited. Option A, claiming a publicly disclosed vulnerability is no longer a genuine concern, inverts the actual risk dynamic: public disclosure increases real-world exploitation risk for systems that remain unpatched, as the vulnerability becomes more widely known to potential attackers. Option B is unsafe: exploits are often used before they are publicly reported, and disclosure itself helps attackers build one, so waiting for a reported exploit leaves the window open. Option D is wrong: while patches can occasionally introduce operational issues needing careful testing, this does not mean patching always introduces more risk than leaving a known, actively targeted vulnerability unaddressed.

Section D, Cyber risk — patch management as a preventive control · Ref D1c · p3063

Question 49: D Insiders already possess legitimate access and knowledge of the organisation's systems and data, meaning many external-facing technical defences (such as firewalls) are not designed to prevent this kind of authorised-access misuse

Insider threat is often considered particularly challenging because insiders already possess legitimate access and detailed knowledge of the organisation's systems, data and processes — many external-facing technical defences, such as firewalls designed to keep unauthorised outsiders out, are not designed to prevent someone with already-authorised access from misusing that access, meaning insider threat requires a different set of controls, such as monitoring of unusual data access patterns, data loss prevention tools, and appropriately restricted access rights aligned to genuine business need (the principle of least privilege). Describing insider threat as not a genuine risk category ignores well-documented cases, including the kind of deliberate data exfiltration described in this scenario, where legitimate access was misused to cause genuine harm. Firewall configuration alone is not sufficient to address insider threat, given that insiders already operate from within the trusted network perimeter that firewalls are primarily designed to protect against external intrusion — additional controls specifically addressing insider risk are needed. Insider threat is a relevant risk consideration for organisations of varying sizes with employees who have system or data access, not confined to very small organisations — indeed, larger organisations with more extensive workforces and more complex access structures often face a larger overall insider threat surface.

Section D, Cyber risk — insider threat as a distinct risk category · Ref D1d · p3064

Question 50: A A Trojan disguises itself as legitimate software to trick installation; a virus self-replicates without needing to disguise itself

This describes a Trojan (or trojan horse) — malware that disguises itself as legitimate, desirable software to trick a user into voluntarily downloading and running it, at which point it delivers its malicious payload. This differs from a virus, which typically self-replicates and spreads by attaching itself to other legitimate files or programs, propagating without necessarily needing to disguise itself as something the user actively wants to install — the deceptive packaging is the defining feature of a Trojan, while self-replication and propagation through infected files is more characteristic of a virus. Treating the two as interchangeable ignores this meaningful distinction in how each type of malware operates and spreads. This scenario is not necessarily ransomware — while a Trojan could be used to deliver ransomware as its payload, a Trojan is defined by its deceptive delivery mechanism, not by any single specific payload type, and not every Trojan delivers ransomware specifically. A Trojan is a category of malicious software, not a network firewall configuration weakness — firewalls are a defensive control that can help prevent certain malware delivery methods, not the malware itself.

Section D, Cyber risk — trojans and disguised malicious software · Ref D1a · p3077

Question 51: B Multi-factor authentication — requiring an additional, independent factor beyond a password means that a compromised password alone is insufficient for an attacker to gain access, since they would also need the second factor

This represents multi-factor authentication (MFA) — requiring an additional, independent authentication factor (here, a one-time code from a separate authenticator app) beyond just a password, which is generally considered significantly more effective than a password alone because a compromised password (obtained through phishing, a data breach elsewhere, or other means) is, by itself, insufficient for an attacker to gain access, since they would also need to obtain the second, independent factor, which is typically much harder to compromise simultaneously with the password, particularly if that second factor requires physical possession of a specific device. This is fundamentally a preventive access control, not exclusively a physical control category — while it may involve a physical device (the authenticator app running on a phone), its classification and function relate to authentication and access control, a broader category than physical controls specifically. It functions primarily as a preventive control, operating before access is granted to stop unauthorised access, not as a purely detective control identifying issues only after an incident has occurred. MFA is widely and consistently recognised as providing substantial additional security benefit compared with password-only authentication, directly contradicting a claim of no meaningful benefit — this is one of the most well-evidenced and commonly recommended cybersecurity controls in practice.

Section D, Cyber risk — multi-factor authentication as a preventive control · Ref D1c · p3078

Question 52: C Supply chain / third-party cyber risk — extending due diligence and security requirements to third parties with system access helps close this gap, since strong internal security can be undermined by a less secure connected third party

This scenario illustrates supply chain or third-party cyber risk — an organisation's own strong internal cybersecurity can be significantly undermined if it grants privileged access to a third party (such as a software vendor for maintenance purposes) whose own security practices are not subject to similarly rigorous scrutiny, since that third party effectively becomes an extension of the organisation's own attack surface, and a security weakness in the vendor's systems could provide an attacker with a route into the organisation's network via that trusted access. Extending due diligence to assess a prospective third party's security practices before granting access, along with ongoing monitoring and contractually specified security requirements throughout the relationship, can help close this gap rather than allowing third-party access to become an unscrutinised weak link. Option A, claiming privileged third-party access has no bearing on the organisation's own cybersecurity exposure directly contradicts well-documented real-world incidents in which exactly this kind of third-party access has served as the entry point for significant breaches. Option B is wrong: while contractual terms are one relevant element of managing this risk, it is not exclusively a legal matter — genuine technical and security-focused practices (due diligence, monitoring, access restriction) are equally important and directly relevant to managing the risk. Option D is wrong: a clean track record does not show that a vendor's current controls are adequate, and due diligence should come before access is granted, not after a breach.

Section D, Cyber risk — supply chain and third-party cyber risk · Ref D1d · p3079

Question 53: D Confidentiality (preventing unauthorised access), Integrity (ensuring information is accurate and unaltered), and Availability (ensuring authorised access when needed)

Information security is commonly structured around three core elements known by the acronym 'CIA': Confidentiality (ensuring information is not disclosed to or accessed by unauthorised individuals), Integrity (ensuring information is accurate, complete and has not been altered without authorisation), and Availability (ensuring information and systems remain accessible to authorised users when they are needed). Different types of cyber attack can be understood as primarily threatening one or more of these three elements — for example, a data breach primarily threatens confidentiality, unauthorised data manipulation threatens integrity, and a denial-of-service attack threatens availability. The CIA acronym in this context has no connection to cost, investment, audit, compliance, insurance or assurance concepts — it specifically and consistently refers to these three information security elements across cybersecurity literature and practice. All three elements are considered equally core and independently relevant to a complete understanding of information security, not merely confidentiality alone.

Section D, Cyber risk — the three core elements of information security · Ref D1a · p3080

Question 54: B Preventive controls cannot guarantee no incident ever occurs; a tested response plan enables faster, more coordinated response

This scenario illustrates a genuine and important gap — even strong preventive controls cannot reduce the probability of a significant cyber incident to zero, given the inherent limitations of any control system and the evolving, adaptive nature of cyber threats, so having a documented, and ideally tested, incident response plan describing roles, communication protocols, containment steps and escalation procedures helps ensure a faster, more coordinated and more effective response if an incident does occur, reducing confusion, wasted time, and ultimately the eventual impact and cost of the incident compared with responding reactively with no pre-agreed plan in place. Option A, claiming sufficiently strong preventive controls make any incident completely impossible, ignores the well-recognised inherent limitations of any control system, which apply equally to cybersecurity controls. Option C misunderstands the purpose: the entire value of incident response planning lies in having the plan prepared in advance of an incident, precisely so that the organisation is not trying to develop a coordinated response for the first time while already under the pressure of a live incident — describing advance planning as providing no benefit misunderstands its whole purpose. Option D is wrong because a significant incident needs decisions and actions well beyond IT, such as senior management escalation, communication with customers and regulators, legal advice and business continuity, so the plan must be organisation-wide.

Section D, Cyber risk — incident response planning and preparedness · Ref D1d · p3082

Question 55: D A zero-day vulnerability — no patch exists yet, so organisations must rely on monitoring and broader defences, not patching alone

This describes a zero-day vulnerability — a previously unknown software vulnerability that is discovered and, in this case, actively exploited by attackers before the software vendor itself is aware of it, meaning there has been 'zero days' during which a patch could have been developed and applied. This is particularly challenging to defend against precisely because, by definition, no patch or official fix yet exists at the point it is first exploited, meaning organisations cannot rely on the patch management approach (discussed in relation to known vulnerabilities) as their primary defence, and must instead depend on broader, complementary defensive measures such as monitoring for unusual system behaviour that might indicate exploitation, network segmentation to limit potential damage, and rapid incident response capability, since prevention through patching alone is not available for a vulnerability that is not yet known or patched. This is fundamentally different from a known vulnerability, for which a patch may already be available — the entire distinguishing feature of a zero-day is the absence of an available fix at the time of exploitation. It is not a physical security weakness — zero-day vulnerabilities are specifically a software or systems security concept, unrelated to physical facility access. While zero-day vulnerabilities are indeed challenging, organisations are not without any means of mitigation — layered defensive measures beyond patching alone, as described, can still reduce the risk and impact of a zero-day exploitation attempt.

Section D, Cyber risk — zero-day vulnerabilities · Ref D1a · p3100

Question 56: B Incident response plans need to explicitly incorporate awareness of applicable notification deadlines and requirements, since failing to notify within the required timeframe can itself result in additional regulatory penalties on top of any consequences of the breach itself

Because many data protection regulatory regimes impose specific, often quite short, timeframes for notifying a regulator (and in some cases affected individuals) after becoming aware of a significant data breach, incident response plans need to explicitly incorporate awareness of these applicable notification deadlines and requirements as part of the planned response, since failing to notify within the required timeframe can itself trigger additional regulatory penalties or scrutiny, layered on top of whatever direct consequences the breach itself has already caused — meaning notification timing is not a peripheral afterthought but a genuine, time-critical element of incident response that needs to be planned for in advance. Claiming notification requirements have no bearing on incident response planning ignores this direct, well-established connection between regulatory notification obligations and how an incident response plan needs to be structured and executed under real time pressure. These notification requirements typically apply broadly across many industries and sectors that hold personal data subject to the relevant data protection regime, not confined to the technology sector specifically. Planning for notification requirements in advance, before any specific incident occurs, is precisely the value of incorporating this into the incident response plan — waiting until after an incident is already fully resolved to consider notification requirements would risk missing the notification deadline entirely, since regulatory notification is often required promptly after becoming aware of a breach, well before full resolution of the underlying incident.

Section D, Cyber risk — regulatory notification requirements following a data breach · Ref D1d · p3102

Question 57: B Network segmentation — it limits the potential spread and impact of a successful compromise by containing it within the affected segment, rather than allowing an attacker who breaches one part of the network to move freely across the entire network to reach more sensitive systems

This represents network segmentation — dividing a network into separate segments so that a compromise of one segment does not automatically grant access to other segments, meaning that if an attacker successfully breaches a less sensitive segment (such as guest Wi-Fi), segmentation limits their ability to then move laterally across the network to reach more sensitive segments (such as finance systems), containing the potential spread and impact of the compromise rather than allowing an attacker who has breached any single point to roam freely across the organisation's entire network. This is a technical network security control, not exclusively a physical control — while it involves network architecture design, its function and classification relate to technical containment of network-based threats, distinct from restricting physical access to tangible facilities. It is not an authorisation control, which concerns approval before a specific transaction or action, a different control mechanism entirely from network architecture design limiting lateral movement. Network segmentation is a well-established and widely recommended control specifically because it does meaningfully limit how far a successful attacker can move within a network — describing it as having no effect on lateral movement directly contradicts its well-documented, core containment function and purpose.

Section D, Cyber risk — network segmentation as a containment strategy · Ref D1c · p3118

Question 58: B A watering hole attack — compromising a website frequented by the intended target group, rather than attacking the target directly, exploiting the trust the target places in a familiar, regularly visited site

This describes a watering hole attack — named by analogy to a predator waiting at a watering hole frequented by its prey, this technique involves compromising a third-party website known to be frequented by the intended target group, rather than attacking the target organisation's own systems directly, exploiting the trust employees place in a familiar, regularly visited site that they would not treat with the same suspicion as an unfamiliar or obviously unsolicited communication. This is not a denial-of-service attack, which aims to overwhelm system capacity to deny availability, a fundamentally different objective from covertly infecting visitors to a compromised third-party site. It is not ransomware, a distinct malware category and objective (file encryption and extortion) unrelated to the watering hole delivery mechanism itself. While SQL injection could potentially be one technique used to actually compromise the third-party website in the first place, a watering hole attack is defined by its overall strategic approach — targeting a frequented third-party site rather than the target directly — not by any single specific compromise technique, and it is not automatically or exclusively classified as SQL injection regardless of the actual method used.

Section D, Cyber risk — watering hole attacks targeting specific victim groups · Ref D1a · p3142

Question 59: A 0.2

Using simple expected value, the expected number of services compromised is the number of services multiplied by the probability of compromise per service: 4 x 0.05 = 0.2. Simple expected value gives 0.2 services, but it does not capture the specific danger of reuse: because the same password is used everywhere, a breach of any one service exposes the credentials for all four, so the impact of a single breach is multiplied. 4 simply restates the number of services on its own, without applying the probability. 5 does not correspond to a correctly applied step of the calculation. 0.05 simply restates the per-service probability, without multiplying by the number of services over which the password is reused.

Section D, Expected exposure from password reuse across services · Ref D1a · p3169

Question 60: A £270,000

The estimated revenue lost is the number of hours the site was offline multiplied by the average revenue generated per hour while operating normally: 6 x £45,000 = £270,000. This figure represents only the direct revenue impact of the outage and would typically be considered alongside other costs, such as reputational damage or customer attrition, when assessing the full cost of the attack. £45,000 simply restates the hourly revenue figure on its own, as if the outage lasted only one hour. £51,000 does not follow from a correct calculation: the hours must be multiplied by the hourly revenue, not added to it. £7,500 would result from dividing the hourly revenue by the number of hours rather than multiplying.

Section D, Quantifying revenue lost from a denial-of-service attack · Ref D1a · p3170