THE CSFR
(CYBER SCHEME FOUNDATIONS; RISK)

EXAM QUESTIONS

CONTENTS

INTRODUCTION

SOURCES OF THE QUESTIONS

FORMAT OF THE EXAM

MULTIPLE CHOICE QUESTIONS

UKCSC MULTIPLE CHOICE QUESTIONS

SHORT FORM QUESTIONS

INTRODUCTION

This document provides the exam questions for The Cyber Scheme's Foundation in Cyber Security Risk Management.

There are two forms of question:

- Multiple choice questions (MCQ).
- Short-form written answers (SF).

A combination of these formats ensures the delegate's knowledge is tested as widely as possible. The two types of question test the delegates in the following ways:

- Recognition Vs Recall – MCQs primarily test recognition. A student must identify the correct answer from a provided list. Short-form answers require free recall. A student must retrieve the information from memory, or appropriate sources without external cues.
- Levels of Thinking – MCQs test lower-order cognitive skills. These include knowledge, identification, and basic application. Short-form written answers demand higher-order cognitive processing. Students must analyse, synthesize, and organize their thoughts to formulate an original response.
- Cueing Effect – MCQs introduce a "cueing effect," where the presence of the correct answer can trigger a student's memory or allow them to arrive at the solution by eliminating obviously incorrect distractors. Short answers eliminate this effect.

Sources of the questions

All questions have been sourced from the following locations:

- The course material
- ISO27005 documentation
- NIST 800-30 documentation
- FAIR Documentation.

Format of the Exam

Participants complete a 90-minute examination comprising multiple-choice and short-form written questions on the afternoon of the final day. The assessment is designed to evaluate understanding of the course content and the ability to apply cyber risk management concepts in practice.

MULTIPLE-CHOICE QUESTIONS

SELECT ONE ANSWER FOR EACH QUESTION.

MODULE ONE

Question 1

What definition of risk is given by the International Standards Organisation?

A. Anything that happens unexpectedly

B. The effect of uncertainty on objectives

C. The effect of the business plan on activity

D. The uncertainty of life.

Question 2

What ISO Document gives the definition of risk?

A. ISO27001

B. ISO27005

C. ISO3000

D. ISO3001.

Question 3

In information security, what is the primary asset you want to protect?

A. Data

B. Equipment

C. People

D. Money.

Question 4

Which of the following is not a secondary asset?

A. Data

B. Equipment

C. People

D. Money.

Question 5

In your risk assessment what would you describe a personal computer as?

A. A primary asset

B. An infrastructure component

C. An asset container

D. A secondary asset.

Question 6

The five elements of risk are?

A. Materials, Threat, Vulnerability, Likelihood, and impact

B. Assets, Threats, Vulnerability, Likelihood, Cost

C. Assets, Threats, Vulnerability, Likelihood, Impact

D. Assets, Threats, Weaknesses, Likelihood, Impact.

Question 7

In assessing risk what would you identify malware as?

A. Threat

B. Vulnerability

C. Weakness

D. Attack vector.

Question 8

When assessing risk, what would you consider an unpatched operating system to be?

A. A Weakness

B. A Threat

C. A Vulnerability

D. An Asset.

Question 9

What would be an example of an impact of a risk?

A. The business loses £1 million

B. The CEO disciplines the CIO

C. The Board vote to increase the cyber security budget

D. The staff bonus is not paid that year.

Question 10

What four elements need to be present for there to be a cyber security risk?

A. Assets, vulnerabilities, Likelihood, impact

B. Threats, vulnerabilities, Likelihood, impact

C. People, Process, Technology, Metrics

D. Assets, Processes, Vulnerabilities, Likelihood.

Question 11

What three elements are we assessing risk against?

A. Budget, impact and cost

B. Confidentiality, access and infrastructure

C. Cost, infrastructure and availability

D. Confidentiality, integrity and availability.

Question 12

What would you class as a breach of integrity?

A. Someone accessing a system without permission

B. The unauthorised modification of data

C. The authorised modification of data

D. Exposing the data to an unauthorised person.

Question 13

What would you class as a breach of availability?

A. A system is not available during working hours

B. A system is unavailable due to planned preventative maintenance

C. A system is available as needed

D. A system is available, but unauthorised people cannot access it.

Question 14

What would you class as a breach of confidentiality?

A. Data is exposed to people in the business who need it to do their jobs

B. Data is exposed to someone outside of the business

C. Data is locked down and only those who need access can see it

D. Anyone in the business can see the data no matter what their job is.

Question 15

A fintech company's board of directors produces a directive saying that the business will not engage in any business ventures that carry a possible regulatory fine of more than £5m. However, the board notes that for innovative blockchain projects they are willing to accept higher operational uncertainties to capture market share. How would you classify this stance?

A. Risk Tolerance

B. Risk Appetite

C. Risk Capacity

D. Risk Threshold.

Question 16

You have found that a business has a significant exposure to a specific cyber risk. The business decides to take out insurance against it. In risk terms what are they doing?

A. Accepting the risk

B. Reducing the risk

C. Eradicating the risk

D. Transferring the risk.

Question 17

A business is made aware of a cyber security risk. They decide to invest in some equipment to help mitigate the risk. In risk terms what are they doing?

A. Accepting the risk

B. Reducing the risk

C. Eradicating the risk

D. Transferring the risk.

Question 18

A business finds a risk but decide there is nothing that can be done about it. In risk terms what are they doing?

A. Accepting the risk

B. Reducing the risk

C. Eradicating the risk

D. Transferring the risk.

Question 19

How might a business go about eradicating a risk completely?

A. Ignore the risk completely

B. Stop the business process where the risk exists

C. Put in very tight controls to manage the process in a strictly controlled way

D. Increase system monitoring within the process for early identification of issues.

Question 20

What is the definition of risk appetite?

A. Potential loss that an individual or organisation is willing to accept in pursuit of a goal or higher return

B. The amount of risk a business is willing to accept in pursuit of its objectives

C. A loss that a business is willing to accept from a single event

D. Estimate of how many times a specific threat or adverse event is expected to happen within a single year.

Question 21

Which of the following is a method to determine risk appetite?

A. The risk team states a risk level and waits to see the organisation's reaction

B. Look in the business plan. It is a legal requirement to record it

C. Work with the business to assess 'The Crown Jewels' to understand what really matters

D. Work with the junior staff to understand how they work and what risks are generated.

Question 22

Which of the following is not a method to determine risk appetite?

A. C-Suite trade-off workshops

B. Peer and industry benchmarking

C. Tabletop incident exercising

D. Risk estimation.

Question 23

How should you treat legal and regulatory requirements in cyber risk?

A. Treat them as a risk

B. Ignore them, they are the responsibility of the compliance team

C. Include a compliance tracker in the risk assessment

D. Use the industry specifics of ISO/IEC 27000 as a checklist.

Question 24

What is the Computer Misuse Act (1990)?

A. It is a standard to be followed

B. It is a legal requirement

C. It is a regulatory requirement

D. It is a compliance item.

Question 25

Which of the following make up the risk management lifecycle?

A. Plan, Do, Check, Act

B. Plan, Implement, Measure, Resolve

C. Plan, Do, Check, Maintain

D. Plan, Do, Measure, Act.

Question 26

What activity takes place at the Plan phase of the risk management lifecycle?

A. Risk assessment and identification of metrics

B. Risk assessment and identification of improvements

C. Understanding risk appetite

D. Development of data flow diagrams.

Question 27

What activity takes place in the Check phase of the risk management lifecycle?

A. Risk assessment

B. Assessing the effectiveness of applied controls

C. Confirming that all parts of the risk assessment are complete

D. Management of the controls.

Question 28

What happens during the Act phase of the risk management lifecycle?

A. Implement the chosen controls

B. Implement amendments to the controls to make them more effective

C. Conduct a further risk analysis

D. Report on the effectiveness of controls to the board.

Question 29

What is the risk management lifecycle based on?

A. Quality principles

B. An information management system

C. The Deming Wheel

D. Confidentiality, Integrity, and Availability.

MODULE TWO

Question 30

Where will you find a definition of Risk Capacity?

A. In ISO/IEC 27005:2022 – (Information technology - Security techniques - Information security risk management)

B. On the NCSC Website

C. In NIST 800-30

D. In ISO/IEC 73:2009 (Risk management – vocabulary).

Question 31

Where will you find a definition of Risk Appetite?

A. In ISO27005 – (Information technology - Security techniques - Information security risk management)

B. ISO/IEC 31000:2018 (Risk management guidelines)

C. On the NCSC Website

D. In NIST 800-30.

Question 32

Where will you find a definition of Risk Tolerance?

A. In ISO27005 – (Information technology - Security techniques - Information security risk management)

B. ISO/IEC 31000:2018 (Risk management guidelines)

C. ISO/IEC 73:2009 (Risk management – vocabulary)

D. In NIST 800-30.

Question 33

What is the correct definition of "residual risk" in information security risk management?

A. The total amount of risk that exists before any security controls or countermeasures are implemented

B. The remaining level of risk that exists after security controls and risk treatment options have been applied

C. The financial loss an organisation incurs immediately after a data breach or cyberattack occurs

D. The risk that is completely eliminated from an IT system through the use of perfect security measures.

Question 34

When a business makes someone or a part of the organisation responsible for risk, what does it mean?

A. Doing the required work or tasks

B. Being answerable to someone or some part of the organisation for that risk

C. Making sure risk is managed

D. Being responsible for the risk assessment.

Question 35

When someone is accountable for the risks, what does it mean?

A. Doing the required work or tasks

B. They perform the risk assessment

C. They own the risk and are responsible for the outcome

D. They report to the board.

Question 36

Who within a business is usually accountable for risk?

A. The Board

B. Senior Managers

C. Middle Managers

D. Operational Managers

Question 37

Who within a business is usually responsible for risk?

A. Only the Board

B. Only Senior Managers

C. Everyone in the business

D. Only Operational Managers.

Question 38

Clear Governance in the management of risk is important because?

A. It ensures effective management of risk

B. It helps identify who should have the biggest bonuses

C. It helps identify who the senior managers are

D. It minimises the amount of people involved in managing risk.

MODULE THREE

Question 39

What are the two main types of approaches to identifying risk?

A. Quantitative and Qualitative

B. ISO27001 and NIST 800-30

C. FAIR and ISO27006

D. Financial and non-financial.

Question 40

What is the definition of qualitative risk assessment?

A. An approach that uses numerical values to measure risk

B. An approach that is aimed at improving quality of business outcomes

C. An approach that utilised the Deming Quality Cycle

D. An approach that evaluates risks using descriptive categories.

Question 41

What is quantitative risk assessment?

A. An approach that uses numerical values to measure risk

B. An approach that is aimed at reducing costs of business outcomes

C. An approach that utilised the Deming Quantity Cycle

D. An approach that evaluates risks using financial values.

Question 42

In a qualitative risk assessment how are Likelihood and Impact expressed?

A. As financial or probability values

B. As a mix of High, Medium, and Low descriptors and numeric values

C. As High, Medium, and low values

D. As text descriptions.

Question 43

What is the most common size of grid used to identify the High, Medium, and Low Descriptors in a qualitative risk assessment?

A. 6 X 6

B. 12 X 12

C. 4 X 4

D. 3 X 3.

Question 44

What is the main advantage of choosing a qualitative risk assessment approach over a quantitative one?

A. It provides precise mathematical data that is easy to include in budgets

B. It eliminates all forms of human bias and subjectivity

C. It can be completed quicker and requires less complex data to start

D. It guarantees a more accurate calculation of the return on investment (ROI) for security controls.

Question 45

In a qualitative risk assessment, what tool is most commonly used to prioritize risks by mapping their likelihood against their impact?

A. Business Impact Analysis (BIA) questionnaire

B. Monte Carlo simulation model

C. Risk Probability and Impact Matrix (Risk Heat Map)

D. Asset Valuation Ledger.

Question 46

An organisation uses a qualitative scale of 1 to 5 for both Likelihood and Impact. If a specific threat has a Likelihood rating of 4 and an Impact rating of 3, what is its qualitative risk score using a standard multiplicative matrix?

A. 7

B. 12

C. 1.33

D. 43.

Question 47

What is considered the biggest disadvantage or limitation of relying solely on a qualitative risk assessment?

A. The results are subjective and depend on the personal opinions and biases of the assessors

B. It requires highly specialised, expensive statistical software to interpret the results

C. It cannot be used with information security risk management frameworks such as ISO 27005

D. It forces organisations to assign an exact financial value to intangible assets such as brand reputation.

Question 48

During a qualitative risk assessment workshop, two department heads strongly disagree on whether a threat's impact should be rated as "Medium" or "High." Which of the following is the best way to resolve this subjectivity?

A. Average the two scores and create a new "Medium-High" category on the fly

B. Use a quantitative formula to calculate the exact financial loss down to the penny

C. Refer to pre-defined, organisational criteria that map descriptive scales to specific operational consequences (e.g., "High" equals downtime over 24 hours)

D. Allow the department head with the larger corporate budget to make the final decision.

Question 49

A Cyber Security Risk Register should contain what?

A. Details of all the business risks faced by the business

B. Details of the residual risks

C. A plan of how risks will be managed

D. Details of the equipment being used to record the risks.

Question 50

Who within the business has to accept any residual risk?

A. The Senior Management Team

B. The Operational Management

C. The Board

D. External stakeholders.

Question 51

If a database server has a Single Loss Expectancy (SLE) of £5,000 and the threat of ransomware is expected to successfully hit the server once every five years, what is the Annualised Loss Expectancy (ALE)?

A. £1,000

B. £2,500

C. £5,000

D. £25,000.

Question 52

In quantitative risk assessment, what is the primary objective of calculating the Annualised Loss Expectancy (ALE) in a quantitative risk assessment?

A. To determine the maximum amount of insurance coverage the company should buy

B. To pinpoint the exact technical vulnerability in a firewall configuration

C. To justify the cost of implementing a security control by comparing it to the financial risk mitigated

D. To calculate the total replacement value of all physical IT hardware.

Question 53

What is considered the most significant challenge or drawback when an organisation attempts a purely quantitative risk assessment?

A. Senior executives generally prefer descriptive words like "High" over financial figures

B. It requires massive amounts of accurate historical data, which is often difficult or impossible to obtain for new threats

C. It cannot be used to measure risk for physical infrastructure or data centres

D. The formulas are subjective and depend heavily on the personal feelings of the risk assessor.

Question 54

How can using statistical techniques such as Monte Carlo simulation improve quantitative risk analysis?

A. It baffles the leadership with science, leading to reduced questions

B. It can produce a range of probabilities, which better informs decision making

C. It is much easier to do than a standard qualitative approach

D. It is extremely accurate.

Question 55

What is one of the key characteristics of Monte Carlo simulation?

A. It is simple to use

B. There are lots of simple to use tools for it on the market

C. It removes doubt

D. It uses random sampling to produce a range of outcomes, rather than a single predicted result

Question 56

What is a Loss Exceedance Curve?

A. A heat map of cyber risk

B. A graph showing the chances of operational, or financial loss over time

C. A statistical chart showing risk within a specific part of a business

D. A risk register used in qualitative risk analysis.

Question 57

When would a Loss Exceedance Curve be used?

A. As a part of qualitative risk assessment

B. As a part of quantitative risk assessment

C. Within a corporate risk register

D. As a part of compliance.

MODULE FOUR

Question 58

What is the Mitre Attack Matrix?

A. It is an online reference of common threats faced by businesses

B. It is a matrix of common risks faced by businesses

C. It is a risk management approach

D. It is a common impact faced by businesses.

Question 59

What does STRIDE stand for?

A. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of privilege

B. Spoofing, Tracking, Research, Intelligence, Defence, Evidence

C. Scenarios, Tampering Research, Intelligence, Defence, Evidence

D. Spoofing, Tampering, Removal, Intelligence, Defence, Evidence.

Question 60

What is STRIDE?

A. A risk management framework

B. A threat assessment tool

C. A tool for prioritising and presenting risk

D. A tool for compiling an organisation's asset register.

Question 61

What does the STRIDE threat modelling approach help an organisation to identify?

A. The financial cost of implementing cyber security controls

B. Potential categories of threats that could affect a system

C. The number of users who should have access to a system

D. The maturity level of an organisation's cyber security programme.

Question 62

Which of the following is NOT one of the STRIDE threat categories?

A. Spoofing

B. Tampering

C. Encryption

D. Repudiation.

Question 63

When using STRIDE, what will help to identify the system trust boundaries?

A. Knowing where the firewalls are located

B. Knowing who the organisation's trusted partners are

C. Developing Data Flow Diagrams

D. Talking to the IT Department.

Question 64

What are Data Flow Diagrams used for?

A. To show the physical location of IT equipment

B. To document an organisation's cyber security policies

C. To show how data moves between processes, systems, data stores, and external entities

D. To calculate the financial impact of a cyber-attack.

Question 65

When using a Data Flow Diagram for threat modelling, which element would represent a database or other location where data is stored?

A. External Entity

B. Data Flow

C. Process

D. Data Store.

Question 66

At what stage in a system lifecycle is it best to do Threat Analysis?

A. Design stage

B. Operational stage

C. Just before the system enters operation

D. It doesn't really matter.

Question 67

What is an advantage of doing Threat Analysis at the design stage?

A. It is quicker

B. It is more thorough

C. It is easier

D. Security can be built in (Secure by Design).

Question 68

From the following options, which is the most reliable source of threat information?

A. The NCSC

B. Wikipedia

C. ChatGPT

D. The Free Security Report.

MODULE FIVE

Question 69

What was the UK Cyber Security Bill meant to achieve?

A. A complete overhaul of the UK Cyber Defences

B. Greater penalties for breaking the law

C. Better management of personal data

D. More security standards.

Question 70

Which of these is not a Legislation concerning IT systems?

A. The Equality Act 2010

B. Health and Safety at Work Act 1974

C. Children Act 1989

D. Computer Misuse Act 1990.

Question 71

How should we treat Legislation in a risk management setting?

A. Treat it as a risk

B. Ignore it, they will be dealt with by compliance

C. Ensure we follow each requirement

D. They do not affect risk management.

Question 72

How should we treat regulations as a part of risk?

A. They do not affect risk management

B. Ignore it, they will be dealt with by compliance

C. Treat them as a risk

D. Ensure we follow each requirement.

Question 73

What is a regulation?

A. An official rule or directive maintained by a recognised authority

B. A law to be followed exactly

C. A code of practice

D. A policy to be followed.

Question 74

What is the definition of legislation?

A. Official rules of the country

B. a law or a set of laws written and passed by parliament

C. Regulations for operating a business

D. EU Directives.

Question 75

What are standards?

A. An ethical system that allows businesses to judge their flaws

B. A level of perfection achieved exactly once by the business, used exclusively to set a benchmark

C. Requirements, specifications, guidelines, or characteristics for repeated use, ensuring materials, products, processes, and services are fit for their purpose

D. A collective agreement among competing companies to make things the same.

Question 76

How would you classify ISO27001?

A. A regulation

B. A standard

C. Legislation

D. Policy.

Question 77

What is a policy?

A. A statement of intention

B. A statement of how to do something

C. The description of a regulation

D. A statement of how a regulation will affect a business.

Question 78

What is a procedure?

A. A statement of intention

B. A statement of how to do something

C. The description of a regulation

D. A statement of how a regulation will affect a business.

Question 79

How would you define the Computer Misuse Act 1990?

A. Policy

B. Regulations

C. Legislation

D. Procedure.

Question 80

What is the core purpose of a Policy?

A. To direct business activity

B. Set rules, boundaries, and corporate intent

C. Provide operational steps to fulfil rules

D. High-level strategy objectives.

Question 81

What is the core purpose of a policy?

A. Set rules, boundaries, and corporate intent

B. Provide operational steps to fulfil rules

C. High-level strategy objectives

D. Present detailed lists, bullet points, or checklists.

Question 82

An organisation discovers a direct conflict between an internal cyber security policy and a national data privacy law. According to the standard hierarchy of governance, which instrument takes precedence?

A. The internal cyber security policy, because internal rules always override external ones.

B. The national data privacy law, because statutory legislation overrides internal governance

C. The industry standard, because technical frameworks override corporate policies

D. The corporate procedure, because operational execution overrides national legislation.

MODULE SIX

Question 83

From the answers provided, what is a common cause of information security failures?

A. Malicious staff

B. Poor training

C. Security being considered outside of the design phase

D. Poor governance structures.

Question 84

Who owns the legal responsibility for risk?

A. The Executive Management

B. The Board

C. The risk and compliance function

D. Operational Management.

Question 85

Where should the cyber risk register reside?

A. As part of the organisation's main risk register

B. With the Chief Information Security Officer (CISO)

C. With risk and compliance

D. With the Board.

Question 86

If an organisation has an internal audit team, what would be a good role for them to play in managing the cyber risk?

A. Conducting the risk assessments

B. Reporting to the board on whether risk management is working effectively

C. Reporting to the risk and compliance team about whether risk management is working effectively

D. Coordinating the risk management activities.

Question 87

Ideally, who should the Risk and Audit Committee report to?

A. The Executive Management Team

B. Operational Management

C. Internal Audit

D. The Board.

Question 88

What is the purpose of managing risk?

A. To understand and manage uncertainty that could affect objectives

B. To ensure obligations and requirements are met

C. To understand what a business is required to do and when

D. To stop anything unexpected happening.

Question 89

What is compliance meant to do?

A. Manage uncertainty

B. Ensure obligations and requirements are met

C. To understand what a business is required to do and when

D. Check everything is being done right.

Question 90

An organisation is reviewing its corporate governance framework. Which statement best describes the difference between risk management and the compliance function?

A. Risk focuses on meeting external legal obligations, whereas compliance focuses on minimising internal operational failures

B. Risk focuses on optimising strategic opportunities, whereas compliance focuses on eliminating financial market volatility

C. Risk focuses on managing the uncertainty of future events, whereas compliance focuses on adhering to established laws and rules

D. Risk focuses on enforcing internal policies, whereas compliance focuses on identifying external competitors

Question 91

A company decides to launch a new mobile app but discovers that the encryption method they are using does not meet the new government data protection laws. At the same time, they become aware that a competitor may launch a similar app first. How should these two issues be categorised?

A. The encryption problem is a compliance issue, and the competitor product is a risk

B. The encryption issue is a risk, and the competitor launch is a compliance issue

C. Both the encryption problem and the competitor are compliance issues

D. Both the encryption problem and the competitor are risk issues.

Question 92

If an organisation is compliant, are they secure?

A. If they have been certified compliant by an independent body

B. If they are compliant with ISO/IEC 31000

C. Compliance does not necessarily mean secure

D. If they maintain their compliance at least annually.

Question 93

When should an organisation undertake a risk assessment?

A. At least annually

B. At least quarterly

C. At least annually, before any significant change in the organisation, or after an incident

D. When the Risk Committee says so.

MODULE SEVEN

Question 94

Which of the following is a recognised risk management framework?

A. ISO/IEC27005

B. NIST 600

C. Fairy

D. Guess.

Question 95

An organisation is implementing the ISO/IEC27005 framework to manage its information risk. During which phase of the risk management process would they establish risk criteria (such as risk evaluation, and risk acceptance) be formally established?

A. Plan

B. Do

C. Check

D. Act.

Question 96

In the ISO/IEC27005 standard, which risk treatment option involves a conscious documented decision to retain the potential loss from a risk because it falls within the organisation's risk criteria?

A. Risk Reduction

B. Risk Avoidance

C. Risk Transfer

D. Risk Acceptance.

Question 97

The FAIR framework breaks down information risk into two primary components. What are these components?

A. Threat capability and vulnerabilities

B. Loss event frequency and size of loss

C. Contact Frequency and Probability of Action

D. Primary Loss and Secondary Loss.

MODULE EIGHT

Question 98

What does the R in SMART stand for?

A. Reassured

B. Reveal

C. Remedial

D. Relevant.

Question 99

SMART is used for developing?

A. Metrics to assess the effectiveness of mitigations

B. Risk mitigation options

C. Risk categories

D. Risk mitigation categories.

Question 100

Which of the following would count as a SMART objective?

A. We need to train employees about phishing

B. Reduce the business's Phishing simulation click- through rate from 20% to 4% in six months

C. Reduce Phishing click-through to zero in six months

D. The organisation will get no Phishing emails by September.

Question 101

In thinking of the Plan, Do, Check, Act cycle, when should SMART objectives be set?

A. Plan

B. Do

C. Check

D. Act.

Question 102

In thinking of the Plan, Do, Check, Act cycle, when should SMART objectives be evaluated?

A. Plan

B. Do

C. Check

D. Act.

Question 103

From the answers provided, in systems architecture what is influenced by understanding risk?

A. The boards stance on risk

B. Defence-in-Depth

C. Risk management options

D. The organisation's maturity.

Question 104

How might the risk assessment influence Disaster Recovery?

A. Disaster recovery plans can be simple, because risks are low

B. The organisation's "crown jewels" are identified and this may need to be recovered first

C. The assets will be valued

D. Layers of defence can be developed reducing downtime.

Question 105

How may the management of staff and their use of systems be influenced by risk assessment?

A. We can identify potentially rogue staff

B. We can identify staff who are ineffective

C. We can identify the types of access staff need to the business systems

D. We can identify the staff that are more likely to make mistakes.

ADDITIONAL QUESTIONS

Question 106

What is the primary purpose of establishing the context during the initial phase of risk management?

A. To determine the definitive financial value of all corporate operational assets

B. To determine the definitive scope of the work

C. To choose the specific software tools that will automate the assessment workflow

D. To bypass qualitative metrics and jump straight into quantitative modelling.

Question 107

In risk management terminology, what is the fundamental difference between a hazard and a risk?

A. A hazard is a consequence, whereas a risk is the probability of financial recovery

B. A hazard is a source of potential harm, whereas a risk is the combination of its likelihood and severity

C. A hazard applies only to physical infrastructure, whereas a risk applies exclusively to digital data

D. A hazard is calculated quantitatively, whereas a risk is evaluated purely through gut instinct.

Question 108

During a structured risk identification workshop, what is the primary objective of establishing a formal 'Risk Taxonomy' across the enterprise?

A. To automatically calculate the precise monetary impact of any identified loss

B. To ensure uniform classification, consistent terminology, and comprehensive coverage of risk types

C. To explicitly assign liability to specific department heads before an event occurs

D. To limit the total number of risk items logged within the central repository.

Question 109

What is the key differentiator between a 'Threat' and a 'Vulnerability' within an information security risk assessment framework?

A. A threat is an internal organisational weakness, whereas a vulnerability is an external force

B. A threat is a potential cause of an unwanted incident, while a vulnerability is a weakness that makes the threat possible

C. Threats are measured qualitatively, while vulnerabilities must always be calculated quantitatively

D. A threat represents a realised financial loss, whereas a vulnerability is a theoretical calculation.

Question 110

What is the primary operational advantage of using a quantitative Monte Carlo simulation over a qualitative 5x5 probability-impact matrix?

A. It eliminates the need to gather inputs from human subject matter experts entirely

B. It outputs a range of probabilistic financial outcomes rather than subjective ordinal rankings

C. It is significantly faster to execute and requires zero technical computation tools

D. It guarantees absolute certainty regarding the exact day a major threat event will manifest.

Question 111

How does an organisation's 'Risk Appetite' differ fundamentally from its 'Risk Tolerance'?

A. Appetite is the absolute maximum loss limit before bankruptcy; tolerance is the ideal goal

B. Appetite is the broad level of risk an organisation is willing to accept to pursue value, while tolerance is the specific variance around a target metric

C. Appetite applies strictly to legal and compliance matters; tolerance applies only to technical systems

D. Appetite is set by operational supervisors; tolerance is approved exclusively by regulators.

Question 112

A risk assessment shows that a critical database has a high-risk rating. The organisation decides to evaluate the 'Inherent Risk' level of this asset. What does this mean?

A. The risk score calculated after implementing all planned compensating security controls

B. The baseline risk level assuming no internal controls or mitigation strategies are active

C. The residual financial risk transferred out to an insurance underwriter

D. The structural vulnerabilities identified exclusively in legacy third-party open-source code.

Question 113

During a risk evaluation session, a risk exceeds the established risk appetite but falls below the risk capacity. What is the required management action?

A. No action is required since the risk is safely within the overall corporate capacity limit

B. The risk must immediately be transferred to an insurance company without further internal review

C. The risk team must attempt to bring it in line with the risk appetite or escalate to the board for an exception

D. The risk appetite statement must be altered immediately to match the current risk level.

Question 114

What does a Business Impact Analysis (BIA) output that directly informs Incident Management and Disaster Recovery?

A. A complete list of Firewall rules and network topologies

B. Recovery Priorities

C. The estimated annual budget allocated for cyber security training modules

D. Background check records for third-party suppliers.

Question 115

An e-commerce firm decides to stop selling products in a specific country due to unstable local regulatory shifts and high fraud rates. Which risk response strategy was executed?

A. Risk Reduction

B. Risk Avoidance

C. Risk Transfer

D. Risk Acceptance.

Question 116

An organisation purchases a cyber liability insurance policy to cover a potential data breach. This action is classified as which type of risk treatment?

A. Risk Reduction

B. Risk Avoidance

C. Risk Transfer

D. Risk Exploitation.

Question 117

An organisation cannot implement multi-factor authentication (MFA) on a legacy accounting mainframe. They decide to restrict network access via strict IP whitelisting and isolate the terminal. These steps are examples of:

A. Risk Reduction

B. Risk Transfer

C. Inherent controls

D. Risk Avoidance.

Question 118

When calculating the financial justification for a proposed control, which condition indicates that a control is economically viable?

A. The cost of the control is equal to the Inherent Annualised Loss Expectancy

B. The reduction in Annualised Loss Expectancy (ALE) is greater than the annual cost of the control

C. The control completely eliminates the risk, reducing the ALE to zero

D. The implementation cost matches the exact replacement cost of the target hardware asset

Question 119

What is residual risk?

A. The total unmitigated risk profile calculated before any internal controls are applied

B. The remaining risk exposure after risk treatment strategies and internal controls have been implemented

C. The financial value recovered from assets following a major disaster event

D. The cost overhead spent maintaining safety systems year over year.

Question 120

Who is the most appropriate individual to assign as a 'Risk Owner' for an operational risk identified inside a business unit?

A. The junior IT support technician who monitors daily system uptime logs

B. The external regulatory auditor responsible for periodic industry validation

C. The business unit leader who manages the budget and has authority over the target process

D. The Chief Risk Officer (CRO), who must personally own every individual operational risk.

Question 121

An enterprise risk dashboard tracks Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs). What is the primary difference between these metrics?

A. KPIs track historical compliance, whereas KRIs predict future financial profits

B. KPIs measure progress toward strategic goals, while KRIs provide early warning signs of rising risk exposures

C. KPIs are designed for external regulators; KRIs are exclusively used by technical engineers

D. KPIs measure qualitative risks, whereas KRIs measure quantitative risks.

Question 122

A risk register is a core document in risk monitoring. How frequently should a standard corporate risk register be updated to ensure operational utility?

A. Exactly once every three years during external certification renewals

B. Continuously or dynamically as new threats emerge, controls fail, or major system changes occur

C. Only when a catastrophic breach or major financial loss event occurs

D. Whenever a new member joins the board of directors.

Question 123

Which metric would serve as the most effective leading Key Risk Indicator (KRI) for predicting potential internal data leakage incidents?

A. The total financial fine paid to regulators last quarter for data compliance failures

B. The percentage of employees who failed or clicked links during unannounced quarterly phishing tests

C. The number of years the company's chief information officer has been in their role

D. The average internet download speed recorded across remote branch offices.

Question 124

An organisation experiences zero security incidents over a twelve-month period. What conclusion should a risk manager draw from this data during monitoring?

A. The organisation's risk profile is zero, and all security spending can be safely halted

B. Controls are working, but the threat landscape must still be monitored as lack of incidents does not prove absence of risk

C. The system is entirely impervious to external state-sponsored threat actors

D. The risk register can be archived and closed out permanently.

Question 125

In risk management, what is the main purpose of linking specific risks to distinct corporate strategic objectives?

A. To ensure that any technical IT failure triggers an automatic alert to the CEO's personal mobile device

B. To help prioritise risk remediation by showing exactly which business goals are threatened by specific exposures

C. To reduce the total amount of liability insurance premiums paid by the legal department

D. To automate the generation of quarterly financial tax returns.

Question 126

What is a primary principle of the ISO/IEC 31000 Risk Management Standard?

A. Risk management must be treated as a separate, isolated task distinct from main business actions

B. Risk management is an integral part of all organisational activities, creating and protecting value

C. Quantitative financial calculations are the only valid way to assess risk

D. Every risk item logged must be completely removed within twelve calendar months.

Question 127

What is the primary role of a 'Risk Management Committee' at the board of directors' level?

A. Reviewing daily network alerts and applying software updates to individual computers

B. Setting strategic risk appetite, reviewing aggregate profiles, and ensuring risk alignment with business goals

C. Writing code for proprietary automated trading platforms

D. Managing employee payroll distributions and tax withholding schedules.

Question 128

Which of the following is an example of an asset?

A. A phishing attack

B. A vulnerability

C. Customer Data

D. A security control.

Question 129

What is the purpose of a risk assessment?

A. To identify and understand risks

B. To purchase new computers

C. To employ more IT staff

D. To remove all risks.

Question 130

Which three areas are commonly considered when assessing cyber security risk?

A. Threat, vulnerability, and impact

B. Password, printer, and email

C. People, Process, and Technology

D. Budget, salary, and profit.

Question 131

What is risk likelihood?

A. How expensive a risk is

B. How likely it is that a risk will occur

C. How many people work for an organisation

D. How long a system has existed.

Question 132

What does risk impact describe?

A. How quickly an attack happens

B. The potential consequences if the risk occurs

C. The number of security controls

D. The age of the computer system.

Question 133

Which of the following is a common risk treatment option?

A. Avoid the risk

B. Ignore the risk

C. Hide the risk

D. Delete the risk register.

Question 134

What does risk acceptance mean?

A. The organisation knowingly agrees to retain the risk

B. The organisation has eliminated the risk

C. The risk has never been identified

D. The organisation has transferred the risk to IT.

Question 135

What does risk avoidance mean?

A. Changing something so that the risk no longer applies

B. Accepting the risk without action

C. Recording the risk in a spreadsheet

D. Buying more insurance.

Question 136

What does risk transfer mean?

A. Sharing or transferring some of the consequences of a risk to another party

B. Deleting the risk

C. Increasing the risk

D. Ignoring the risk.

Question 137

Which of the following is an example of risk transfer?

A. Changing a password

B. Installing a Firewall

C. Taking out insurance

D. Removing a vulnerable server.

Question 138

Which of the following is an example of a preventative control?

A. Incident report

B. Firewall

C. A business asset

D. A vulnerability.

Question 139

What is risk ownership?

A. Taking responsibility for ensuring a risk is appropriately managed

B. Owning the computer affected by the risk

C. Paying for all security controls personally

D. Writing the risk assessment software.

Question 140

What is phishing?

A. An attempt to trick someone into providing information or performing an action

B. A type of firewall

C. A backup technique

D. A method of encrypting files.

Question 141

Which of the following is part of the CIA triad?

A. Accounting

B. Intelligence

C. Confidentiality

D. Administration.

Question 142

Why should risk decisions be documented?

A. To provide evidence of what was decided and why

B. To make the risk register look complicated

C. To prevent risks from changing

D. To avoid having security controls.

Question 143

What is the purpose of a risk assessment methodology?

A. To guarantee that no risks exist

B. To provide a consistent approach to identifying and assessing risks

C. To replace business management

D. To prevent employees accessing computers.

Question 144

Why is it important to identify assets during risk assessment?

A. Assets automatically remove vulnerabilities

B. Assets prevent cyber-attacks

C. You need to understand what could be affected by a risk

D. Assets replace risk controls.

Question 145

If a risk has a high likelihood and high impact, how would it normally be treated?

A. It would normally be ignored

B. It would be deleted from the risk register

C. It would automatically be accepted

D. It would usually receive significant attention.

Question 146

What is quantitative risk assessment?

A. Using only words such as High and Low

B. Asking employees for their opinions only

C. Uses numerical or financial values to estimate risk

D. Counting vulnerabilities without considering impact.

Question 147

What does integrity mean?

A. Information is available 24 hours a day

B. Information remains accurate and has not been improperly altered

C. Everyone can access information

D. Information is always encrypted.

Question 148

What does confidentiality mean?

A. Information is always available

B. Information cannot be changed

C. Information is automatically backed up

D. Information is only accessible to authorised people.

Question 149

What is a data breach?

A. A scheduled software update

B. A normal backup

C. An incident where information is accessed, disclosed or lost without authorisation

D. A password change.

Question 150

Why should risks be reviewed regularly?

A. It makes the risk register longer

B. Risks, threats and business circumstances can change

C. It removes the need for security controls

D. Risks never change.

Question 151

In cyber risk management, how do threats and vulnerabilities differ?

A. A vulnerability is a weakness in a system, while a threat is a potential danger or event that could exploit that weakness

B. A threat is an accidental event caused by an employee, while a vulnerability is an intentional attack by an outsider

C. A threat is a physical hazard like a power outage, while a vulnerability is strictly a software glitch

D. A vulnerability is an external attacker, while a threat is the internal impact of an attack.

Question 152

Which of the following best describes the process of "Risk Identification" in a cyber security program?

A. Purchasing insurance to cover the financial costs of a potential cyberattack

B. Installing antivirus software and firewalls on all company computers to block malware

C. Finding and listing all information assets (like laptops, servers, and data) and the potential risks they face

D. Deciding that the risk of a minor data breach is acceptable because it is too costly to fix.

Question 153

A company decides to require all employees to use Multi-Factor Authentication (MFA) to access company emails. Which risk treatment strategy does this represent?

A. Risk Avoidance

B. Risk Acceptance

C. Risk Transfer

D. Risk Mitigation

UK CYBER SECURITY COUNCIL QUESTIONS

SELECT ONE ANSWER FOR EACH QUESTION.

Question 1

What does UKCSC stand for?

A. United Kingdom Canoeing Social Clubs

B. United Kingdom Cyber Security Council

C. United Kingdom Cyber Skills Centre

D. United Kingdom Cyber Skills Council.

Question 2

What is the primary purpose of professional registration with the UK Cyber Security Council?

A. To provide access to government cyber security contracts

B. To demonstrate that an individual's competence, professionalism and ethics meet the Council's professional standards

C. To replace all existing cyber security qualifications

D. To provide an alternative to employment references.

Question 3

Which of the following is the correct sequence of professional titles currently awarded by the UK Cyber Security Council, from entry level to the highest level?

A. Associate, Practitioner, Principal, Chartered

B. Foundation, Practitioner, Senior, Chartered

C. Associate, Professional, Senior, Chartered

D. Practitioner, Principal, Fellow, Chartered.

Question 4

For most professional titles, who normally handles an individual's application and assessment?

A. The National Cyber Security Centre (NCSC)

B. The applicant's employer

C. A UK Cyber Security Council Licensed Body

D. The applicant's university.

Question 5

What is the role of the UK Cyber Security Council's Standard for Professional Competence and Commitment?

A. It specifies the minimum salary for cyber security professionals

B. It provides the standard against which professional competence and commitment are assessed

C. It lists approved cyber security software products

D. It provides mandatory technical controls for organisations.

Question 6

Which of the following is a responsibility of a UK Cyber Security Council registrant?

A. Guaranteeing that their employer will never suffer a cyber-attack

B. Maintaining and developing their professional competence

C. Certifying their employer against ISO/IEC 27001

D. Reporting every cyber incident directly to the NCSC.

Question 7

Which statement best describes the CPD obligation for UK Cyber Security Council registrants?

A. CPD is optional once an individual becomes Chartered

B. Only technical training counts as CPD.

C. CPD is mandatory and registrants are expected to plan, undertake and record their development

D. CPD is only required when applying for registration for the first time.

Question 8

What can happen if a registrant fails to meet the requirements for maintaining professional registration?

A. Nothing, because registration is permanent

B. They are automatically moved to the Associate level

C. They can be removed from the Council's Professional Register

D. Their employer is automatically fined.

Question 9

Which of the following best describes the responsibility of a registrant regarding professional ethics?

A. Ethics only apply when the registrant is working for the government

B. The registrant is expected to comply with the Council's ethical requirements and demonstrate professional integrity

C. Ethical responsibilities belong exclusively to the employer

D. Ethics are only assessed when the individual first applies.

Question 10

What happens after an applicant successfully completes the professional registration process through a Licensed Body?

A. The Licensed Body awards the applicant a university degree

B. The applicant's details are uploaded to the Council's Professional Register

C. The applicant automatically becomes an employee of the Council

D. The applicant is exempt from future CPD requirements.

Question 11

Which statement best describes the responsibility of a UK Cyber Security Council registrant after achieving professional registration?

A. Registration demonstrates competence at the date of application but requires no further action

B. The registrant is responsible for maintaining their professional competence, undertaking CPD and continuing to meet professional requirements

C. The registrant only needs to maintain their technical certifications

D. The registrant's employer becomes responsible for maintaining their registration.

SHORT-FORM QUESTIONS

ANSWER EACH QUESTION IN YOUR OWN WORDS.

Question 1

What is cyber security risk? Explain what is meant by risk and how it applies to cyber security.

Answer:

Question 2

Explain the difference between a threat, a vulnerability and a risk. Give a simple cyber security example of a single threat and vulnerability and the associated risk.

Answer:

Question 3

What is a risk appetite, and why is it important to an organisation?

Answer:

Question 4

How can legislation and regulation affect the way an organisation conducts cyber security risk assessments?

Answer:

Question 5

Explain the difference between compliance and risk management. Why should an organisation not rely solely on compliance to manage cyber risk?

Answer:

Question 6

Describe the main stages of a typical risk management lifecycle.

Answer:

Question 7

What are assets, and why are they important when assessing cyber security risk?

Answer:

Question 8

Explain why identifying the business value or criticality of an asset is important when assessing cyber security risk.

Answer:

Question 9

What is a risk owner, and what responsibilities should a risk owner have?

Answer:

Question 10

Name two commonly used cyber security or information security risk management frameworks and briefly explain how one of them can support risk management.

Answer:

Question 11

Explain the difference between responsibility and accountability in relation to cyber security risk.

Answer:

Question 12

What is a risk assessment methodology, and why is it important to use a defined methodology?

Answer:

Question 13

Explain the difference between qualitative and quantitative cyber security risk assessment.

Answer:

Question 14

What is threat analysis, and how does it contribute to a cyber security risk assessment?

Answer:

Question 15

What is the purpose of a threat modelling approach such as STRIDE?

Answer:

Question 16

How can cyber security standards influence an organisation's risk management activities?

Answer:

Question 17

Why might an organisation choose to use ISO 31000 or ISO/IEC 27005 when managing cyber security risk?

Answer:

Question 18

How can cyber security risk influence systems architecture decisions? Give two examples.

Answer:

Question 19

Explain how cyber security risk should influence disaster recovery and business continuity planning.

Answer:

Question 20

How can cyber security risk influence decisions about staff, skills and training?

Answer:

Question 21

An organisation identifies a high risk involving a critical business system. Describe three possible risk treatment options and explain when each might be appropriate.

Answer:

Question 22

Explain how cyber security risk management can support business decision-making rather than simply being a technical security activity.

Answer:

Question 23

Why do human resource policies and staff management decisions play a critical role in managing cyber security risk?

Answer:

Question 24

Briefly describe the four main options an organisation has for treating an identified risk: Accept, Avoid, Mitigate/Reduce, and Transfer.

Answer:

Question 25

What is "residual risk," and how does a risk manager determine if this risk level is acceptable?

Answer: