PassQueen
a.k.a dumpsqueen.com

BCS Foundation Certificate in Information Security Management Principles V9.0

BCS CISMP-V9

Version Demo

Total Demo Questions: 16

Total Premium Questions: 165

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Information Security Management Principles	29
Topic 2, Information Risk	15
Topic 3, Security Frameworks	14
Topic 4, Security Culture	19
Topic 5, Technical Security Controls	63
Topic 6, Incident Management	11
Topic 7, Business Continuity Management	14
Total	165

QUESTION NO: 1

Which of the following types of organisation could be considered the MOST at risk from the theft of electronic based credit card data?

A. Online retailer.

B. Traditional market trader.

C. Mail delivery business.

D. Agricultural producer.

ANSWER: A

Explanation:

Online retailer is correct because its core business model commonly requires it to collect, transmit, process, or store payment-card data through internet-facing websites, payment pages, checkout services, customer accounts, and connected back-end systems. This creates an attractive target for criminals seeking payment-card numbers and associated cardholder data at scale. The risk is heightened by the exposure of public-facing e-commerce applications to threats such as credential attacks, web-skimming scripts, vulnerable software, insecure integrations, and configuration errors. An online retailer must therefore apply security controls throughout the card-data environment, including protection of payment pages, strong access control, secure system configuration, monitoring, and prompt vulnerability management. The Payment Card Industry Data Security Standard provides the baseline security requirements for entities that store, process, or transmit cardholder data, with particular relevance to e-commerce payment flows. The PCI Security Standards Council also publishes specific guidance on protecting online payment pages from e-skimming attacks. These characteristics make an online retailer the organisation most directly exposed to theft of electronic credit-card data. See the PCI DSS overview and the PCI Security Standards Council's e-skimming guidance.

QUESTION NO: 2

In order to maintain the currency of risk countermeasures, how often SHOULD an organisation review these risks?

A. Once defined, they do not need reviewing.

B. A maximum of once every other month.

C. When the next risk audit is due.

D. Risks remain under constant review.

ANSWER: D

Explanation:

"Risks remain under constant review." is correct because risk management is a continual activity, rather than an exercise performed only at fixed intervals. The circumstances that determine a risk's likelihood, impact and treatment can change at any time: business processes may change, new systems or suppliers may be introduced, threats and vulnerabilities may emerge, or an incident may reveal that an existing control is not operating as intended. Maintaining ongoing oversight allows the organisation to identify such changes promptly and determine whether countermeasures remain suitable, effective and proportionate to the current level of risk.

This does not necessarily mean that every risk assessment must be fully repeated every day. Instead, risks should be monitored continuously, with formal reassessment triggered by material changes, incidents, audit results, changes to legal or contractual requirements, and planned periodic review. This approach ensures that the risk register and risk-treatment decisions remain current and that management can respond before residual risk becomes unacceptable. ISO/IEC 27001 requires organisations to perform information-security risk assessments at planned intervals and when significant changes are proposed or occur, which supports continuous monitoring combined with structured reviews. See ISO/IEC 27001 overview and the NCSC risk management guidance.

QUESTION NO: 3

Which standards framework offers a set of IT Service Management best practices to assist organisations in aligning IT service delivery withbusiness goals - including security goals?

A. ITIL.

B. SABSA.

C. COBIT

D. ISAGA.

ANSWER: A

Explanation:

ITIL. is correct because ITIL is a widely adopted best-practice framework for IT service management (ITSM). Its purpose is to help organisations design, deliver, operate, and continually improve IT-enabled services in a way that creates value and supports business objectives. Rather than treating technology as an isolated function, ITIL promotes service management practices that connect service performance, customer and stakeholder needs, governance, risk, resilience, and continual improvement to organisational goals.

Security is an important consideration within this service-management context. ITIL practices support the incorporation of information-security requirements into the lifecycle of services, including service design, change enablement, incident management, supplier management, availability, continuity, and risk management. This helps ensure that security controls and security-related service requirements are planned, implemented, monitored, and improved as part of normal service delivery. ITIL therefore provides the requested set of ITSM best practices for aligning IT service delivery with business goals, including security goals. The official ITIL overview is available from PeopleCert; further service-management guidance is provided by ITIL UK.

QUESTION NO: 4

In a virtualised cloud environment, what component is responsible for the secure separation between guest machines?

A. Guest Manager

B. Hypervisor.

C. Security Engine.

D. OS Kernal

ANSWER: B

Explanation:

The **Hypervisor.** is correct because it is the virtualisation layer that creates, runs and isolates virtual machines (guests) on shared physical hardware. It allocates virtualised processor, memory, storage and network resources to each guest, while enforcing boundaries intended to prevent one guest machine from directly accessing another guest's memory, processing state or virtual devices. This isolation is fundamental to multi-tenancy in cloud environments, where separate customers or workloads can operate on the same underlying host infrastructure.

Secure separation depends on the hypervisor correctly mediating access to physical resources and maintaining distinct virtual-machine execution contexts. Consequently, the hypervisor is a high-value component within the trusted computing base: a weakness or compromise at this layer could affect the isolation guarantees provided to hosted guests. NIST describes the hypervisor as the software layer that enables and manages virtual machines and highlights virtualisation security considerations, including isolation, in NIST SP 800-125. This aligns with the cloud and virtualisation security principles covered by BCS information-security training; see the BCS Certificate in Information Security Management Principles qualification overview.

QUESTION NO: 5

What type of attack attempts to exploit the trust relationship between a user client based browser and server based websites forcing the submission of an authenticated request to a third party site?

A. XSS.

B. Parameter Tampering

C. SQL Injection.

D. CSRF.

ANSWER: D

Explanation:

CSRF is the correct answer because Cross-Site Request Forgery abuses the trust that a target website places in requests received from a user's browser. When a user has already authenticated to a site, their browser commonly retains credentials such as session cookies. An attacker can then cause that browser to submit a crafted request to the authenticated target application, potentially performing an action under the user's identity without their informed intent. The key characteristic is that the request originates from the victim's authenticated browser session and is accepted by the target server as though the user deliberately initiated it. CSRF is particularly relevant to state-changing operations, such as changing account details, creating transactions, or modifying application settings. Effective defences bind requests to the legitimate user interaction, commonly through unpredictable anti-CSRF tokens, validation of request origin where appropriate, and secure cookie settings such as `SameSite`. OWASP describes CSRF as forcing an end user to execute unwanted actions on a web application in which they are currently authenticated, matching the trust-relationship and authenticated-request scenario in the question. See the OWASP CSRF overview and the OWASP CSRF Prevention Cheat Sheet.

QUESTION NO: 6

What advantage does the delivery of online security training material have over the distribution of printed media?

A. Updating online material requires a single edit. Printed material needs to be distributed physically.

B. Online training material is intrinsically more accurate than printed material.

C. Printed material is a 'discoverable record' and could expose the organisation to litigation in the event of an incident.

D. Online material is protected by international digital copyright legislation across most territories.

ANSWER: A

Explanation:

"Updating online material requires a single edit. Printed material needs to be distributed physically." is correct because centrally hosted training can be amended once and then made available immediately to every learner who accesses the current version. This is especially valuable in information security, where policies, threat examples, reporting contacts, legal requirements, and technical controls can change quickly. A central learning platform also helps an organisation present a consistent, current message to its workforce rather than relying on multiple copies held in different locations.

The practical benefit is not simply that training is electronic; it is that ownership and version control can be managed centrally. Following an update, the organisation can withdraw or replace obsolete content, notify users of the revision, and require completion of the revised module where appropriate. This reduces the time, cost, and administrative effort involved in producing replacement copies and physically delivering them to all intended recipients. NIST's guidance on awareness and training recognises the need for security awareness material to be maintained and updated as organisational and risk conditions change. See NIST SP 800-50: Building an Information Technology Security Awareness and Training Program and the NCSC's 10 Steps to Cyber Security.

QUESTION NO: 7

Which of the following acronyms covers the real-time analysis of security alerts generated by applications and network hardware?

A. CERT

B. SIEM.

C. CISM.

D. DDoS.

ANSWER: B

Explanation:

SIEM is the correct acronym because Security Information and Event Management platforms collect, centralise, correlate, and analyse security-relevant event data from many sources, including applications, operating systems, network devices, security appliances, and cloud services. A key SIEM capability is near-real-time monitoring: it ingests logs and alerts as they are produced, applies correlation rules and analytics to identify potentially significant patterns, and presents prioritised alerts to security personnel for investigation and response. This supports the operational detection activities expected in an information-security management environment, where isolated events may be benign but a combination of events can indicate an attack or policy breach.

In practice, SIEM tooling provides a consolidated view of security activity, helping an organisation retain and search event records while also detecting suspicious behaviour quickly enough to support incident handling. NIST describes security information and event management as a log-management capability that can support event correlation and monitoring, while Microsoft explains how SIEM systems aggregate and analyse security data for threat detection. See NIST SP 800-92: Guide to Computer Security Log Management and Microsoft Sentinel SIEM overview.

QUESTION NO: 8

What physical security control would be used to broadcast false emanations to mask the presence of true electromagentic emanations from genuine computing equipment?

A. Faraday cage.

B. Unshielded cabling.

C. Copper infused windows.

D. White noise generation.

ANSWER: D

Explanation:

White noise generation is the appropriate control because it deliberately emits random electromagnetic energy to obscure the meaningful, unintentional electromagnetic signals produced by computing equipment. This is a form of emissions-security protection: an attacker attempting to collect and reconstruct information from compromising emanations encounters a much noisier signal environment, making detection, isolation, and interpretation of the genuine emissions substantially more difficult. In this context, “white noise” means broadly distributed random interference used as a masking signal; it is not limited to audible sound. The control is particularly relevant where sensitive information may be processed and where an organisation’s risk assessment identifies a realistic risk of technical surveillance or electromagnetic eavesdropping. It should be selected, installed, and tested as part of a proportionate, defence-in-depth physical-security design, alongside appropriate equipment placement, cabling decisions, and any necessary shielding measures. NIST describes TEMPEST as addressing the protection of information-processing equipment from compromising emanations, which provides the relevant security context for this control. NIST physical and environmental protection guidance also recognises the need to address information leakage from equipment and communications paths. See the NIST TEMPEST glossary entry and NIST SP 800-53 PE-19, Information Leakage.

QUESTION NO: 9

Which of the following is NOT an accepted classification of security controls?

A. Nominative.

B. Preventive.

C. Detective.

D. Corrective.

ANSWER: A

Explanation:

“Nominative.” is the correct choice because it is not a recognised functional classification for information-security controls. Security controls are commonly classified according to the purpose they serve in managing risk. Established functional categories include preventive controls, which reduce the likelihood of an unwanted event occurring; detective controls, which identify events or conditions that have occurred; and corrective controls, which limit impact and restore an acceptable state after an incident. These categories help organisations select a balanced set of safeguards rather than relying on a single type of protection.

This classification approach is consistent with recognised information-security practice. For example, NIST describes controls in terms of their role in preventing, detecting, responding to, and recovering from adverse events, while the UK National Cyber Security Centre explains that effective cyber security requires controls that reduce risk and support detection and response. “Nominative” relates to naming or designation in ordinary language; it does not describe a security-control function and is not used as an accepted control category in CISMP security-management principles. See NIST SP 800-53 Rev. 5 and NCSC 10 Steps to Cyber Security.

QUESTION NO: 10

You are undertaking a qualitative risk assessment of a likely security threat to an information system.

What is the MAIN issue with this type of risk assessment?

A. These risk assessments are largely subjective and require agreement on rankings beforehand.

B. Dealing with statistical and other numeric data can often be hard to interpret. C. There needs to be a large amount of previous data to "train" a qualitative risk methodology.

C. It requires the use of complex software tools to undertake this risk assessment.

ANSWER: A

Explanation:

These risk assessments are largely subjective and require agreement on rankings beforehand. Qualitative assessment expresses likelihood and impact using descriptive scales, such as low, medium, and high, rather than measured numerical values. Its value therefore depends on participants sharing a clear, documented understanding of what each ranking means. For example, the organisation must establish thresholds for what constitutes a “high” likelihood and a “major” business impact, and should apply these consistently across risks.

Professional judgement from system owners, security specialists, and business stakeholders is essential when evidence is incomplete or cannot be meaningfully quantified. However, different people can reasonably interpret descriptive terms differently, based on their experience, risk appetite, and knowledge of the affected service. Agreeing rating definitions, assessment criteria, and the risk matrix in advance reduces this variability and makes prioritisation more consistent, repeatable, and defensible. NIST notes that qualitative assessments use non-numerical categories and that their results can be influenced by the assessor’s judgement; the method should therefore be supported by defined scales and criteria. See NIST SP 800-30 Rev. 1 and NCSC risk-management guidance.

QUESTION NO: 11

A business impact analysis identifies that a payroll system must be restored within four hours following a major disruption.

Which business continuity measure has been identified?

A. Recovery Point Objective (RPO).

B. Recovery Time Objective (RTO).

C. Maximum Tolerable Period of Disruption.

D. Service Level Agreement.

ANSWER: B

Explanation:

Recovery Time Objective (RTO). is correct because it specifies the maximum acceptable period of time that a service may remain unavailable following an interruption. In this case, the payroll system must be recovered and made available within four hours.

An RTO is used to determine the urgency and design of recovery arrangements, such as the required recovery solution, availability of alternative facilities, restoration procedures, staffing, and testing frequency. It is distinct from a Recovery Point Objective, which concerns the maximum acceptable amount of data loss measured in time. NIST describes the recovery time objective as the maximum allowable downtime for an information system resource following a disruption. See NIST SP 800-34 Rev. 1, Contingency Planning Guide.

QUESTION NO: 12

When an organisation decides to operate on the public cloud, what does it lose?

A. The right to audit and monitor access to its information.

B. Control over Intellectual Property Rights relating to its applications.

C. Physical access to the servers hosting its information.

D. The ability to determine in which geographies the information is stored.

ANSWER: C

Explanation:

Operating in the public cloud means the organisation no longer has physical access to the servers hosting its information. The cloud service provider owns, operates, and secures the data-centre facilities and the underlying hardware. Customers consume compute, storage, and networking as managed services through consoles, APIs, and contractual arrangements rather than by entering the data centre or directly handling the equipment on which their workloads run.

This is a fundamental feature of the public-cloud delivery model: physical infrastructure is pooled and managed by the provider for multiple customers. The customer retains responsibility for, and control of, its data, identities, configurations, and the security settings available within the service, but it does not control physical access to the provider's server estate. This separation is reflected in the shared-responsibility model, under which the provider is responsible for security *of* the cloud, including facilities and physical infrastructure. The UK National Cyber Security Centre explains the importance of understanding these provider and customer responsibilities when using cloud services: NCSC Cloud Security Principles. AWS also describes physical infrastructure and facilities as provider responsibilities in its Shared Responsibility Model.

QUESTION NO: 13

What form of risk assessment is MOST LIKELY to provide objective support for a security

Return on Investment case?

A. ISO/IEC 27001.

B. Qualitative.

C. CPNI.

D. Quantitative

ANSWER: D

Explanation:

Quantitative is correct because it expresses risk in numerical and financial terms, giving decision-makers measurable evidence for an information-security investment case. A quantitative assessment estimates variables such as the probability or frequency of a threat event, the financial impact of a successful event, and the resulting expected loss. These values can be compared with the cost of a proposed safeguard and its expected reduction in loss exposure. This supports calculations such as annualised loss expectancy, cost-benefit analysis, and return on investment, making the rationale for expenditure more objective, transparent, and suitable for business approval.

For example, if an organisation can estimate the expected annual financial loss from a particular cyber incident and quantify the reduction achieved by a control, it can compare the avoided loss with the control's implementation and operating costs. Although estimates and assumptions still require careful validation, using monetary values provides a clearer business-oriented basis for prioritising security investments. NIST describes quantitative risk analysis as using numerical values and notes that risk assessment informs risk-response decisions; see NIST SP 800-30 Rev. 1. ISO also explains that ISO 31000 provides principles and guidance for managing risk and supporting organisational decision-making; see ISO 31000 risk management.

QUESTION NO: 14

A security analyst has been asked to provide a triple A service (AAA) for both wireless and remote access network services in an organization and must avoid using proprietary solutions.

What technology SHOULD they adapt?

A. TACACS+

B. RADIUS.

C. Oauth.

D. MS Access Database.

ANSWER: B

Explanation:

RADIUS is the appropriate technology because it is an open, standard AAA protocol designed to centralise network-access control. AAA comprises authentication, which verifies a user or device identity; authorisation, which returns the access permissions or policy attributes applicable to that identity; and accounting, which records session activity for operational monitoring, auditing, and charging purposes where required.

For wireless access, a wireless access point or controller can act as a RADIUS client and submit user or device credentials to a central RADIUS server, commonly as part of enterprise Wi-Fi access control. For remote access, a VPN or network-access server can use the same RADIUS service to authenticate users and apply centrally managed access policy. This enables consistent identity checking, access decisions, and session logging across both types of service rather than maintaining separate local credential stores.

RADIUS is defined through IETF standards and is implemented by many independent network, security, and identity-management suppliers. It therefore supports the requirement to avoid vendor-proprietary technology while retaining interoperability between access devices and an AAA server. RFC 2865 specifies RADIUS authentication and authorisation behaviour, while RFC 2866 specifies RADIUS accounting: RFC 2865 and RFC 2866.

QUESTION NO: 15

What is the MAIN security benefit of using multi-factor authentication for remote access?

A. A stolen password alone is less likely to allow unauthorised access.

B. It removes the need to manage user identities.

C. It guarantees that remote devices are free from malware.

D. It allows users to share accounts securely.

ANSWER: A

Explanation:

A stolen password alone is less likely to allow unauthorised access. is correct because multi-factor authentication requires evidence from two or more different factor types, such as something the user knows, something the user has, or something the user is. An attacker who obtains a password through phishing, credential reuse, or a data breach will therefore usually need an additional factor before access can be granted.

Multi-factor authentication is particularly valuable for remote access because internet-facing authentication services are frequent targets for password attacks. The factors must be genuinely distinct; entering two passwords does not provide multi-factor authentication. Organisations should select authentication methods appropriate to the risk, protect recovery processes, and monitor authentication activity for signs of compromise. The NCSC recommends multi-factor authentication as an important protection for corporate online services: NCSC guidance on multi-factor authentication.

QUESTION NO: 16

Which of the following testing methodologies TYPICALLY involves code analysis in an offline environment without ever actually executing thecode?

A. Dynamic Testing.

B. Static Testing.

C. User Testing.

D. Penetration Testing.

ANSWER: B

Explanation:

Static Testing. is correct because static testing examines software artefacts without running the program. The artefacts may include source code, design documents, configuration files, requirements, architecture diagrams, and build settings. In an information-security context, static code analysis tools and manual code reviews inspect the codebase offline to identify potentially insecure patterns, such as unsafe functions, inadequate input validation, hard-coded credentials, or risky data handling. Because the application is not executed, this approach can be used early in the development lifecycle and can identify issues before a test deployment is available.

This is commonly described as static application security testing (SAST). SAST analyses an application “from the inside out” by reviewing its source, bytecode, or binaries rather than observing behaviour during execution. It supports secure development by helping teams remediate weaknesses close to the point at which they are introduced. The UK National Cyber Security Centre discusses incorporating security testing and code review into secure development practices: NCSC Developers Collection. OWASP also provides guidance on source-code review and static analysis within its testing framework: OWASP Web Security Testing Guide.