PassQueen
a.k.a dumpsqueen.com

Certificate in Cybersecurity Analysis (CCA)

IIBA IIBA-CCA

Version Demo

Total Demo Questions: 9

Total Premium Questions: 94

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

The process by which organizations assess the data they hold and the level of protection it should be given based on its risk to loss or harm from disclosure, is known as:

A. vulnerability assessment.

B. internal audit.

C. information classification.

D. information categorization.

ANSWER: C

Explanation:

information classification. is the process of evaluating information according to its sensitivity and the potential business, legal, privacy, operational, or reputational harm that could result if it is disclosed, altered, lost, or otherwise improperly handled. The organization then assigns a classification label—such as public, internal, confidential, or restricted—and defines the handling protections associated with that label. Those protections commonly include access restrictions, encryption, approved storage and transmission methods, retention requirements, and secure disposal procedures.

The wording focuses on the data the organization holds and on determining the appropriate degree of protection according to disclosure-related risk. That is the central purpose of an information-classification scheme: it creates a repeatable, risk-based basis for applying proportionate safeguards to information assets. Classification also enables cybersecurity analysts and business stakeholders to identify where sensitive information resides, communicate its handling requirements, and ensure that security controls are aligned with the information's value and sensitivity throughout its lifecycle.

This approach is consistent with the NIST guidance that defines information classification as assigning information to classes based on protection requirements and cites the sensitivity of information as a key consideration. See the NIST definition of information classification and NIST's FIPS 199 security categorization standard.

QUESTION NO: 2

What risk to information integrity is a Business Analyst aiming to minimize, by defining processes and procedures that describe interrelations between data sets in a data warehouse implementation?

A. Unauthorized Access

B. Confidentiality

C. Data Aggregation

D. Cross-Site Scripting

ANSWER: C

Explanation:

Data Aggregation is correct because a data warehouse brings together information from multiple operational sources, often with different structures, definitions, timing, and levels of detail. The relationships among those data sets must be explicitly defined through such measures as data models, business rules, source-to-target mappings, lineage, transformation logic, and reconciliation procedures. These controls help ensure that combined data remains meaningful, accurate, and consistent when it is summarized or analyzed. Without a clear understanding of how data sets relate, users could aggregate incompatible records, double-count values, apply an incorrect join, or draw conclusions from data that has lost its intended business context. A Business Analyst helps minimize this risk by eliciting and documenting the rules that govern how data is integrated and used, allowing stakeholders to rely on warehouse outputs for decisions. This supports the core concept of data integrity: preserving the accuracy, consistency, and reliability of information throughout its lifecycle. See the NIST definition of data integrity and IIBA's overview of the Certificate in Cybersecurity Analysis.

QUESTION NO: 3

Which of the following should be addressed by functional security requirements?

A. System reliability

B. User privileges

C. Identified vulnerabilities

D. Performance and stability

ANSWER: B

Explanation:

User privileges should be addressed by functional security requirements because privileges define security behavior that the solution must perform and enforce. A requirement may specify that the system assign permissions through defined roles, restrict access to authorized resources and actions, prevent users from performing activities outside their authority, and revoke or adjust access when a user's responsibilities change. These are observable capabilities that can be designed, implemented, tested, and traced to security objectives.

Analyzing privileges also supports fundamental security principles such as least privilege, separation of duties, and controlled use of elevated permissions. For example, a requirement could state that only authorized administrators may change account permissions, that privileged actions require additional authentication, or that privileged activity must be recorded for review. These requirements express what the system must do to protect information and enforce access policy.

NIST's access-control guidance identifies account management, access enforcement, least privilege, separation of duties, and privileged accounts as core control areas, directly supporting the need to specify privilege-related security functionality. See NIST SP 800-53 Rev. 5 and its Access Control control family.

QUESTION NO: 4

An organization is replacing a legacy application. The legacy application uses a shared service account to send files to three downstream systems. Why should this integration be examined during cybersecurity analysis of the replacement?

A. To preserve the shared service account without changing its permissions

B. To identify security impacts to connected systems, access rights, and data flows

C. To document the legacy application's user-interface screens

D. To establish the delivery schedule for the replacement project

ANSWER: B

Explanation:

The integration should be examined because the replacement may change trust relationships, authentication methods, permissions, and data flows across the connected systems. A shared service account may have broad access and can make accountability difficult. Understanding the current integration enables the analyst to identify security impacts and define requirements for an appropriate future-state identity, authorization, and logging approach.

The purpose is not merely to preserve the existing account, document application screens, or determine the project delivery schedule. Those activities would not address the security exposure created by the shared integration credential and connected systems.

QUESTION NO: 5

Public & Private key pairs are an example of what technology?

A. Virtual Private Network

B. IoT

C. Encryption

D. Network Segregation

ANSWER: C

Explanation:

Encryption is correct because public and private key pairs are the defining mechanism of asymmetric cryptography, also called public-key cryptography. In this approach, an entity has a mathematically related key pair: the public key may be distributed to others, while the private key is protected by its owner. A party can encrypt information using the recipient's public key so that only the corresponding private key can decrypt it. This supports confidentiality without requiring the parties to have previously exchanged a shared secret.

Key pairs also enable digital signatures. The owner uses the private key to sign information, and recipients use the associated public key to validate the signature. When appropriate cryptographic algorithms, key protection, and certificate practices are used, this provides evidence of the signer's identity and detects changes to signed content. Public-key encryption and digital signatures are foundational controls for technologies such as TLS, certificate-based authentication, secure email, and code signing. NIST describes public-key cryptography as using two related keys, with one public and the other private, for cryptographic operations. See NIST's definition of public-key cryptography and its Digital Signature Standard.

QUESTION NO: 6

What common mitigation tool is used for directly handling or treating cyber risks?

A. Exit Strategy

B. Standards

C. Control

D. Business Continuity Plan

ANSWER: C

Explanation:

Control is the common mitigation tool used to directly handle, or treat, cyber risks. In risk management, treatment means selecting and implementing measures that modify risk by reducing the likelihood of a threat event, reducing its impact, or both. A control is the specific safeguard that produces this result in practice. For example, multifactor authentication can reduce the likelihood of unauthorized account access; encryption can reduce the impact of data exposure; and logging with monitoring can support timely detection and response. Controls may be technical, administrative, or physical, and an effective risk treatment plan identifies the control, its intended risk-reduction outcome, the responsible owner, and how its effectiveness will be monitored.

This use of controls aligns with established cybersecurity risk guidance. NIST defines controls as safeguards or countermeasures prescribed to protect the confidentiality, integrity, and availability of information systems and their information. The NIST Cybersecurity Framework also organizes risk-management activities around selecting and implementing appropriate safeguards to manage cybersecurity risk. Accordingly, when an analyst identifies a cyber risk and needs a direct mechanism to mitigate it, a control is the appropriate tool to specify and apply. See NIST's definition of a control and the NIST Cybersecurity Framework.

QUESTION NO: 7

What things must be identified to define an attack vector?

A. The platform, application, and data

B. The attacker and the vulnerability

C. The system, transport protocol, and target

D. The source, processor, and content

ANSWER: B

Explanation:

The attacker and the vulnerability is correct because an attack vector is understood as the path or means through which a threat actor exploits a weakness to achieve an unauthorized outcome. Identifying the attacker establishes the threat source involved in the scenario. This may be an external criminal, malicious insider, opportunistic attacker, automated botnet, or another source with relevant intent and capability. Identifying the vulnerability establishes the exploitable condition that makes the route viable, such as an unpatched software flaw, insecure configuration, weak credentials, overly broad privileges, or susceptible user behavior.

Together, these elements define a meaningful cybersecurity analysis scenario: a particular threat source can exploit a particular weakness through a feasible route. This lets an analyst assess likelihood, understand the exposure, identify affected assets and controls, and recommend proportionate treatments such as remediation, stronger authentication, access restrictions, monitoring, or user awareness measures. NIST describes an attack vector as the means by which an attacker gains access to a system or network, reinforcing the connection between the threat actor and the exploitable route. This framing also supports the risk-based analysis expected in cybersecurity work. See the NIST definition of attack vector and IIBA's Certificate in Cybersecurity Analysis overview.

QUESTION NO: 8

Which of the following is a cybersecurity risk that should be addressed by business analysis during solution development?

A. Project budgets may prevent developers from implementing the full set of security measures

B. QA may fail to identify all possible security vulnerabilities during system testing

C. The solution may not be understood well enough to reliably identify security risks

D. Code may be implemented in ways that introduce new vulnerabilities

ANSWER: C

Explanation:

The solution may not be understood well enough to reliably identify security risks is the cybersecurity risk most directly addressed through business analysis. During solution development, business analysis establishes a sufficiently complete shared understanding of the business objective, stakeholders, user roles, workflows, data handled, external interfaces, and applicable constraints. This context enables the team to identify security-relevant assets, data flows, trust boundaries, potential misuse scenarios, and security requirements before technical design and implementation decisions become difficult or costly to change.

Cybersecurity analysis is therefore not limited to documenting functional requirements. It includes eliciting and clarifying non-functional requirements such as identity and access management, least-privilege authorization, confidentiality, integrity, audit logging, data retention, privacy, and regulatory obligations. Accurate process and data-flow understanding also provides essential input to threat modeling, allowing appropriate controls to be incorporated into the solution design. This is consistent with secure-by-design practices, which integrate security considerations throughout the development lifecycle rather than treating them as a late testing activity. NIST's Secure Software Development Framework identifies security requirements and risk-informed practices as activities to integrate into software development: NIST SP 800-218. Further guidance on incorporating security throughout the system development life cycle is available in NIST SP 800-64 Revision 2.

QUESTION NO: 9

How is a risk score calculated?

A. Based on the confidentiality, integrity, and availability characteristics of the system

B. Based on the combination of probability and impact

C. Based on past experience regarding the risk

D. Based on an assessment of threats by the cyber security team

ANSWER: B

Explanation:

A risk score is calculated based on the combination of probability and impact. This approach expresses risk as the relationship between the likelihood that a threat event will occur and the magnitude of the resulting consequences to the organization. Many risk methodologies implement this relationship as likelihood multiplied by impact, while others use qualitative scales—such as low, medium, and high—and a risk matrix to map the two ratings to an overall score or risk level.

Probability considers the chance of the scenario occurring in the organization's specific environment. Relevant inputs can include threat capability and intent, exposure, vulnerability exploitability, existing control effectiveness, and relevant historical information. Impact evaluates the potential business harm if the scenario occurs, including operational disruption, financial loss, regulatory or legal consequences, reputational effects, and damage involving information confidentiality, integrity, or availability.

Combining these dimensions permits consistent prioritization: a scenario must be evaluated both for its chance of occurring and for the seriousness of its potential outcome. This supports proportionate selection and treatment of cybersecurity risks. NIST's risk-management guidance describes risk in terms of the likelihood of threat events and adverse impacts, while ISO 31000 defines risk as the effect of uncertainty on objectives. See NIST SP 800-30 Rev. 1 and ISO 31000:2018.