ISC2 CSSLP - Quiz Questions with Answers

Domain 1: Secure Software Concepts

1.

An organization is concerned about leaks of confidential data to systems that are not cleared for it. It should focus on developing rules that prevent which of the following?

Write-down

Read-up

Write-up

Read-down

Correct answer: Write-down

*Bell-LaPadula is a confidentiality protection model that combines attributes of Mandatory Access Control (MAC) and Discretionary Access Control (DAC). Its Simple Security Rule prevents reading data at a higher level of classification ("read up"), while its * property prevents writing data to a system with a lower classification level ("write down").*

Biba is an integrity model designed to protect higher-level, more trustworthy data from being corrupted by lower-level data. Its no write-up rule blocks systems from writing data to a system with a higher classification level. Its second rule states that a system reading/processing data from a lower-level system ("read down") will have its integrity level lowered as a result.

2.

An organization allows all users to have administrator-level access on their own computers to ensure that they can do their jobs. This is a failure of:

Least privilege

Psychological acceptability

Separation of duties

Fail secure

Correct answer: Least privilege

The principle of least privilege states that users, applications, etc. should only have the access and privileges needed to do their jobs. Most users don't need admin privileges, so this practice creates security risks.

Separation of duties refers to the fact that critical processes (such as approving payments) should be split across multiple people to protect against fraud, social engineering, etc.

Fail secure means that a system should default to a secure state if something goes wrong, rather than an insecure one. For example, magnetic locks on a secure area should be locked if they lose power.

Psychological acceptability indicates that users are more likely to comply with security requirements that are easy to use and transparent.

3.

Single points of failures are MOST closely related to which of the following concepts?

Resiliency

Diversity of Defense

Separation of Duties

Least Common Mechanism

Correct answer: Resiliency

Some of the key security design principles include:

- ***Resiliency:*** *Software systems should be designed to eliminate single points of failure via backups, redundancy, etc. The failure of a single point of failure could render the system unusable or insecure.*
- ***Separation of Duties:*** *Separation of duties or compartmentalization divides high-risk or critical processes across multiple roles. This reduces the probability that a malicious user could carry out the action or be tricked into doing so.*
- ***Least Common Mechanism:*** *Least common mechanism states that different processes with different privilege levels should not use the same function or mechanism because it is more difficult to keep these paths separate. Instead, each process should have its own mechanism.*
- ***Diversity of Defense:*** *Software defenses should be diverse geographically, technically, etc. This reduces the probability that an event affecting one defense will impact all of them.*

4.

An application is configured to drop authentication requests if it becomes overloaded and can't validate them. This is an example of which of the following security best practices?

Fail secure

Economy of mechanism

Least privilege

Least common mechanism

Correct answer: Fail secure

Fail secure means that a system should default to a secure state if something goes wrong rather than an insecure one. Denying access if it can't validate users' identity is an example of fail secure.

The principle of least privilege states that users, applications, etc. should only have the access and privileges needed to do their jobs.

Economy of mechanism (also known as the Keep it Simple principle) states that software design and implementation should be as simple as possible to reduce the risk of errors.

Least common mechanism prevents against sharing mechanisms or functions in code that are used by different users or processes if they have different levels of privilege.

5.

Which of the following principles recommends use of high-quality, secure libraries?

Component Reuse

Least Common Mechanism

Complete Remediation

Economy of Mechanism

Correct answer: Component Reuse

Some of the key security design principles include:

- ***Component Reuse:*** *Don't reinvent the wheel. The use of secure, high-quality components rather than custom code can improve the efficiency and security of software and reduce the attack surface.*
- ***Economy of Mechanism:*** *Economy of Mechanism or "Keep It Simple" states that the design and implementation of software should be as simple as possible. Complex systems have a larger attack surface and are more difficult to troubleshoot if something goes wrong.*
- ***Complete Mediation:*** *Complete mediation states that authorization should be performed for every request, even if requests are repeated. This ensures that the authorization system is never bypassed.*
- ***Least Common Mechanism:*** *Least common mechanism states that different processes with different privilege levels should not use the same function or mechanism because it is more difficult to keep these paths separate. Instead, each process should have its own mechanism.*

6.

An organization wants to ensure that a system containing low-quality data can't corrupt a higher-level system's data. Which of the following types of rules can prevent this?

Write-up

Write-down

Read-up

Read-down

Correct answer: Write-up

*Bell-LaPadula is a confidentiality protection model that combines attributes of Mandatory Access Control (MAC) and Discretionary Access Control (DAC). Its Simple Security Rule prevents reading data at a higher level of classification ("read up"), while its * property prevents writing data to a system with a lower classification level ("write down").*

Biba is an integrity model designed to protect higher-level, more trustworthy data from being corrupted by lower-level data. Its no write-up rule blocks systems from writing data to a system with a higher classification level. Its second rule states that a system reading/processing data from a lower-level system ("read down") will have its integrity level lowered as a result.

7.

Which of the following principles is intended to improve the effectiveness and resiliency of an organization's cyber defenses?

Diversity of Defense

Open Design

Economy of Mechanism

Component Reuse

Correct answer: Diversity of Defense

Some of the key security design principles include:

- ***Diversity of Defense:*** *Software defenses should be diverse geographically, technically, etc. This reduces the probability that an event affecting one defense will impact all of them.*
- ***Economy of Mechanism:*** *Economy of Mechanism or "Keep It Simple" states that the design and implementation of software should be as simple as possible. Complex systems have a larger attack surface and are more difficult to troubleshoot if something goes wrong.*
- ***Open Design:*** *Also known as Kerckhoffs's Principle, the principle of open design states that a system should not rely on security via obscurity. For example, in encryption algorithms the only secret is the secret key, all details of the encryption algorithm used can be known to an attacker without compromising the security of the system.*
- ***Component Reuse:*** *Don't reinvent the wheel. The use of secure, high-quality components rather than custom code can improve the efficiency and security of software and reduce the attack surface.*

8.

Which of the following access control models is MOST likely to use factors such as time of day in its access determinations?

Rule-based access control

Mandatory access control

Discretionary access control

Resource-based access control

Correct answer: Rule-based access control

Several access control models exist, including:

- ***Mandatory Access Control (MAC):*** *MAC centrally controls access to resources based on a combination of sensitivity labels and user clearances. The military Unclassified/Confidential/Secret/Top Secret model with compartments is an example of a MAC system.*
- ***Discretionary Access Control (DAC):*** *DAC uses the concepts of users and groups and allows users to define who can access their resources. DAC is commonly used by computers, such as Linux's support for granting read/write/execute permissions to the owner, group, members, and others.*
- ***Role-Based Access Control (RBAC):*** *Role-based access control assigns each user with a role and a set of associated permissions, which are used to determine if a request is valid. For example, a software developer may have access to certain systems and tools, while a software manager may have access to HR information that the developer cannot access.*
- ***Rule-Based Access Control (RBAC):*** *Rule-based access control uses access control lists (ACLs) and Boolean logic to determine if a request is valid. For example, rules may restrict the times during which a system can be accessed or the devices permitted to access sensitive data.*
- ***Attribute-Based Access Control (ABAC):*** *ABAC assigns attributes to a user's identity that are used to determine their access. For example, a developer may have a certain set of permissions on one system but a different set on another.*
- ***Resource-Based Access Control (RBAC):*** *Resource-based access control systems include the Impersonation and Delegation Model used by Kerberos and the Trusted Subsystem Model. Under the Impersonation and Delegation Model, one entity delegates its access and privileges to another, allowing the other entity to impersonate it to achieve some task. The Trusted Subsystem Model controls access based on a trusted device rather than a user's identity.*

9.

Which of the following focuses on reducing software's attack surface by minimizing complexity?

Economy of Mechanism

Least Privilege

Least Common Mechanism

Component Reuse

Correct answer: Economy of Mechanism

Some of the key security design principles include:

- ***Economy of Mechanism:*** *Economy of Mechanism or "Keep It Simple" states that the design and implementation of software should be as simple as possible. Complex systems have a larger attack surface and are more difficult to troubleshoot if something goes wrong.*
- ***Least Privilege:*** *Under the Principle of Least Privilege, users are granted the minimum set of permissions necessary to perform their role.*
- ***Least Common Mechanism:*** *Least common mechanism states that different processes with different privilege levels should not use the same function or mechanism because it is more difficult to keep these paths separate. Instead, each process should have its own mechanism.*
- ***Component Reuse:*** *Don't reinvent the wheel. The use of secure, high-quality components rather than custom code can improve the efficiency and security of software and reduce the attack surface.*

10.

Firewalls and access controls are examples of which type of security control?

Preventative

Detective

Responsive

Proactive

Correct answer: Preventative

The three main ways to manage security risks in production include:

- ***Prevention:** Blocking a security incident from occurring. Examples of preventative controls include firewalls, access controls, and encryption.*
- ***Detection:** Identifying a security incident that requires mitigation. Detective controls include audit logs, honeypots, and intrusion detection systems (IDS).*
- ***Response:** Mitigating an identified security incident. Incident response efforts are supported by backups, incident response teams (IRTs), and computer forensics.*

Proactive security actions would involve threat hunting or similar activities.

11.

Which of the following is designed to eliminate single points of failure in security?

Defense in depth

Fail secure

Complete mediation

Least common mechanism

Correct answer: Defense in depth

Defense in depth means that multiple layers of security should be used so that a failure of one layer doesn't leave the system vulnerable.

Fail secure means that a system should default to a secure state if something goes wrong, rather than an insecure one. For example, magnetic locks on a secure area should be locked if they lose power.

Complete mediation ensures that access controls can't be bypassed by checking them on every request, not just the first one.

Least common mechanism prevents against sharing mechanisms or functions in code that are used by different users or processes if they have different levels of privilege.

12.

A program uses cryptography that relies on the attacker not knowing the details of the algorithms used. This is a violation of which of the following?

Open Design

Component Reuse

Psychological Acceptability

Least Common Mechanism

Correct answer: Open Design

Some of the key security design principles include:

- ***Open Design:*** *Also known as Kerckhoffs's Principle, the principle of open design states that a system should not rely on security via obscurity. For example, in encryption algorithms the only secret is the secret key, all details of the encryption algorithm used can be known to an attacker without compromising the security of the system.*
- ***Least Common Mechanism:*** *Least common mechanism states that different processes with different privilege levels should not use the same function or mechanism because it is more difficult to keep these paths separate. Instead, each process should have its own mechanism.*
- ***Psychological Acceptability:*** *If users don't understand a security control or feel that it obstructs their work, they'll attempt to work around it, undermining it. Security functionality should be user-friendly and transparent to the user.*
- ***Component Reuse:*** *Don't reinvent the wheel. The use of secure, high-quality components rather than custom code can improve the efficiency and security of software and reduce the attack surface.*

13.

The military classification system is MOST closely related to which of the following access control models?

MAC

DAC

RBAC

ABAC

Correct answer: MAC

Several access control models exist, including:

- ***Mandatory Access Control (MAC):*** *MAC centrally controls access to resources based on a combination of sensitivity labels and user clearances. The military Unclassified/Confidential/Secret/Top Secret model with compartments is an example of a MAC system.*
- ***Discretionary Access Control (DAC):*** *DAC uses the concepts of users and groups and allows users to define who can access their resources. DAC is commonly used by computers, such as Linux's support for granting read/write/execute permissions to the owner, group, members, and others.*
- ***Role-Based Access Control (RBAC):*** *Role-based access control assigns each user with a role and a set of associated permissions, which are used to determine if a request is valid. For example, a software developer may have access to certain systems and tools, while a software manager may have access to HR information that the developer cannot access.*
- ***Rule-Based Access Control (RBAC):*** *Rule-based access control uses access control lists (ACLs) and Boolean logic to determine if a request is valid. For example, rules may restrict the times during which a system can be accessed or the devices permitted to access sensitive data.*
- ***Attribute-Based Access Control (ABAC):*** *ABAC assigns attributes to a user's identity that are used to determine their access. For example, a developer may have a certain set of permissions on one system but a different set on another.*
- ***Resource-Based Access Control (RBAC):*** *Resource-based access control systems include the Impersonation and Delegation Model used by Kerberos and the Trusted Subsystem Model. Under the Impersonation and Delegation Model, one entity delegates its access and privileges to another, allowing the other entity to impersonate it to achieve some task. The Trusted Subsystem Model controls access based on a trusted device rather than a user's identity.*

14.

A department within a financial institution has data that could be used by another department for insider trading. Which of the following models is BEST suited to protecting against misuse of this data?

Brewer-Nash

Bell-LaPadula

Biba

Clark-Wilson

Correct answer: Brewer-Nash

Brewer-Nash or the Chinese Wall is a confidentiality model for enterprises. It addresses the case where one group within an organization may have information that cannot be shared with another.

*Bell-LaPadula is a confidentiality protection model that combines attributes of Mandatory Access Control (MAC) and Discretionary Access Control (DAC). Its Simple Security Rule prevents reading data at a higher level of classification, while its * property prevents writing data to a system with a lower classification level.*

Biba is an integrity model designed to protect higher-level, more trustworthy data from being corrupted by lower-level data. Its no-write-up rule blocks systems from writing data to a system with a higher classification level. Its second rule states that a system reading/processing data from a lower-level system will have its integrity level lowered as a result.

Clark-Wilson is a transaction-based integrity model that defines Constrained Data Items (CDIs) and Unconstrained Data Items (UDIs). Integrity Verification Processes (IVPs) verify that CDI meets integrity rules for a particular state, and Transformation Processes (TPs) can change CDIs from one valid state to another.

15.

Which of the following limits the damage that a user can do by limiting their access to a system?

Least Privilege

Separation of Duties

Economy of Mechanism

Complete Mediation

Correct answer: Least Privilege

Some of the key security design principles include:

- ***Least Privilege:*** *Under the Principle of Least Privilege, users are granted the minimum set of permissions necessary to perform their role.*
- ***Separation of Duties:*** *Separation of duties or compartmentalization divides high-risk or critical processes across multiple roles. This reduces the probability that a malicious user could carry out the action or be tricked into doing so.*
- ***Economy of Mechanism:*** *Economy of Mechanism or "Keep It Simple" states that the design and implementation of software should be as simple as possible. Complex systems have a larger attack surface and are more difficult to troubleshoot if something goes wrong.*
- ***Complete Mediation:*** *Complete mediation states that authorization should be performed for every request, even if requests are repeated. This ensures that the authorization system is never bypassed.*

16.

Terms like "five nines" are related to which of the following?

Availability

Confidentiality

Integrity

Non-Repudiation

Correct answer: Availability

Some of the core goals of cryptographic algorithms include:

- ***Confidentiality:*** *Protecting sensitive information from being disclosed to unauthorized parties. Confidentiality can be protected overtly (encryption, hashing) or covertly (steganography, digital watermarking).*
- ***Integrity:*** *Preventing data from being modified without authorization. Data integrity can be protected by hash functions, digital signatures, parity bits, and cyclic redundancy checking.*
- ***Availability:*** *Ensuring that authorized personnel can access systems or data. 99.999% uptime is "five nines availability." Load balancing, backups, and redundant systems are examples of solutions for protecting availability.*
- ***Non-Repudiation:*** *Preventing a user from denying that they took a particular action. Digital signatures and the blockchain's immutable ledger are examples of protections against repudiation.*

17.

Factors such as passwords, biometrics, etc. are related to which of the following?

- **Authentication**
- Authorization
- Accountability
- Availability

Correct answer: Authentication

Authentication: *Verifying the identity of the user. Common authentication factors include something you know (passwords, etc.), something you have (smartphone, etc.), and something you are (biometrics).*

Authorization: *Validating that an authenticated user has the right to perform a particular action. Authorization can be managed via various access control models.*

Accountability: *Monitoring and recording activity by users on systems. Audit logs should include at a minimum the user's identity, the action taken, the object acted upon, and the time at which the action was taken.*

Availability: *Ensuring that authorized personnel can access systems or data. Load balancing, backups, and redundant systems are examples of solutions for protecting availability.*

18.

An organization has suffered a Business Email Compromise (BEC) attack in which an employee has been tricked into wiring money to an attacker. Which of the following secure design principles could have prevented this?

Separation of duties

Economy of mechanism

Complete mediation

Fail secure

Correct answer: Separation of duties

Separation of duties refers to the fact that critical processes (such as approving payments) should be split across multiple people to protect against fraud, social engineering, etc.

Economy of mechanism (also known as the Keep it Simple principle) states that software design and implementation should be as simple as possible to reduce the risk of errors.

Complete mediation ensures that access controls can't be bypassed by checking them on every request, not just the first one.

Fail secure means that a system should default to a secure state if something goes wrong, rather than an insecure one. For example, magnetic locks on a secure area should be locked if they lose power.

19.

Which of the following addresses the risk that a particular security control may fail to identify a threat?

Defense in Depth

Resiliency

Component Reuse

Diversity of Defense

Correct answer: Defense in Depth

Some of the key security design principles include:

- ***Defense in Depth:*** *The principle of defense in depth states that assets should be protected by multiple independent layers of security. The use of layered security makes it more difficult for an attacker to bypass or defeat every defense and achieve their objective.*
- ***Resiliency:*** *Software systems should be designed to eliminate single points of failure via backups, redundancy, etc. The failure of a single point of failure could render the system unusable or insecure.*
- ***Component Reuse:*** *Don't reinvent the wheel. The use of secure, high-quality components rather than custom code can improve the efficiency and security of software and reduce the attack surface.*
- ***Diversity of Defense:*** *Software defenses should be diverse geographically, technically, etc. This reduces the probability that an event affecting one defense will impact all of them.*

20.

A website only validates a user when they first visit the site and assumes that all future requests are valid. This is an example of a failure of which of the following?

Complete mediation

Least privilege

Economy of mechanism

Least common mechanism

Correct answer: Complete mediation

Complete mediation ensures that access controls can't be bypassed by checking them on every request, not just the first one. Assuming that follow-on requests are valid creates the potential for bypassing authentication.

The principle of least privilege states that users, applications, etc. should only have the access and privileges needed to do their jobs.

Economy of mechanism (also known as the Keep it Simple principle) states that software design and implementation should be as simple as possible to reduce the risk of errors.

Least common mechanism prevents against sharing mechanisms or functions in code that are used by different users or processes if they have different levels of privilege.

21.

Which of the following is intended to protect against attackers bypassing authentication systems?

Complete Mediation

Least Privilege

Separation of Duties

Defense in Depth

Correct answer: Complete Mediation

Some of the key security design principles include:

- ***Complete Mediation:*** *Complete mediation states that authorization should be performed for every request, even if requests are repeated. This ensures that the authorization system is never bypassed.*
- ***Least Privilege:*** *Under the Principle of Least Privilege, users are granted the minimum set of permissions necessary to perform their role.*
- ***Separation of Duties:*** *Separation of duties or compartmentalization divides high-risk or critical processes across multiple roles. This reduces the probability that a malicious user could carry out the action or be tricked into doing so.*
- ***Defense in Depth:*** *The principle of defense in depth states that assets should be protected by multiple independent layers of security. The use of layered security makes it more difficult for an attacker to bypass or defeat every defense and achieve their objective.*

22.

Which of the following is a common argument FOR using passwords for authentication?

Psychological acceptability

Economy of mechanism

Principle of least privilege

Leveraging existing components

Correct answer: Psychological acceptability

Psychological acceptability indicates that users are more likely to comply with security requirements that are easy to use and transparent. Passwords makes sense to people, which is why they are widely used.

Economy of mechanism (also known as the Keep it Simple principle) states that software design and implementation should be as simple as possible to reduce the risk of errors.

The principle of least privilege states that users, applications, etc. should only have the access and privileges needed to do their jobs.

Leveraging existing components encourages code reuse because it reduces the risk of new vulnerabilities being introduced into software.

23.

An application uses the same code for managing administrative and unprivileged accounts. This is a violation of which of the following?

Least common mechanism

Leveraging existing components

Economy of mechanism

Least privilege

Correct answer: Least common mechanism

Least common mechanism prevents against sharing mechanisms or functions in code that are used by different users or processes if they have different levels of privilege.

Leveraging existing components encourages code reuse because it reduces the risk of new vulnerabilities being introduced into software.

Economy of mechanism (also known as the Keep it Simple principle) states that software design and implementation should be as simple as possible to reduce the risk of errors.

The principle of least privilege states that users, applications, etc. should only have the access and privileges needed to do their jobs.

24.

Which of the following models is designed to prevent corruption of data on more trusted systems by data of lower-level systems?

- **Biba**
- Bell-LaPadula
- Brewer-Nash
- Clark-Wilson

Correct answer: Biba

Biba is an integrity model designed to protect higher-level, more trustworthy data from being corrupted by lower-level data. Its no-write-up rule blocks systems from writing data to a system with a higher classification level. Its second rule states that a system reading/processing data from a lower-level system will have its integrity level lowered as a result.

*Bell-LaPadula is a confidentiality protection model that combines attributes of Mandatory Access Control (MAC) and Discretionary Access Control (DAC). Its Simple Security Rule prevents reading data at a higher level of classification, while its * property prevents writing data to a system with a lower classification level.*

Clark-Wilson is a transaction-based integrity model that defines Constrained Data Items (CDIs) and Unconstrained Data Items (UDIs). Integrity Verification Processes (IVPs) verify that CDI meets integrity rules for a particular state, and Transformation Processes (TPs) can change CDIs from one valid state to another.

Brewer-Nash or the Chinese Wall is a confidentiality model for enterprises. It addresses the case where one group within an organization may have information that cannot be shared with another.

25.

Which of the following is NOT an example of a detective security control?

Firewall

Audit log

Honeypot

Intrusion Detection System (IDS)

Correct answer: Firewall

The three main ways to manage security risks in production include:

- ***Prevention:*** *Blocking a security incident from occurring. Examples of preventative controls include firewalls, access controls, and encryption.*
- ***Detection:*** *Identifying a security incident that requires mitigation. Detective controls include audit logs, honeypots, and intrusion detection systems (IDS).*
- ***Response:*** *Mitigating an identified security incident. Incident response efforts are supported by backups, incident response teams (IRTs), and computer forensics.*

Proactive security actions would involve threat hunting or similar activities.

26.

Which of the following would be MOST applicable to an investigation into a security incident?

Accountability

Authentication

Authorization

Availability

Correct answer: Accountability

Accountability: *Monitoring and recording activity by users on systems. Audit logs should include at a minimum the user's identity, the action taken, the object acted upon, and the time at which the action was taken.*

Authentication: *Verifying the identity of the user. Common authentication factors include something you know (passwords, etc.), something you have (smartphone, etc.), and something you are (biometrics).*

Authorization: *Validating that an authenticated user has the right to perform a particular action. Authorization can be managed via various access control models.*

Availability: *Ensuring that authorized personnel can access systems or data. Load balancing, backups, and redundant systems are examples of solutions for protecting availability.*

27.

The ability to deny that a user took a particular action violates which of the following?

Non-repudiation

Confidentiality

Integrity

Availability

Correct answer: Non-repudiation

Some of the core goals of cryptographic algorithms include:

- ***Confidentiality:*** *Protecting sensitive information from being disclosed to unauthorized parties. Confidentiality can be protected overtly (encryption, hashing) or covertly (steganography, digital watermarking).*
- ***Integrity:*** *Preventing data from being modified without authorization. Data integrity can be protected by hash functions, digital signatures, parity bits, and cyclic redundancy checking.*
- ***Availability:*** *Ensuring that authorized personnel can access systems or data. Load balancing, backups, and redundant systems are examples of solutions for protecting availability.*
- ***Non-Repudiation:*** *Preventing a user from denying that they took a particular action. Digital signatures and the blockchain's immutable ledger are examples of protections against repudiation.*

28.

Which of the following is NOT one of the three types of audit-related risk?

Residual risk

Inherent risk

Detection risk

Control risk

Correct answer: Residual risk

The three forms of audit-related risk are:

- ***Inherent Risk:*** *Risks that are inherent to a particular process or tool that should be managed by security controls.*
- ***Detection Risk:*** *The risk that a potential issue will be undetected by an audit, causing a potential issue.*
- ***Control Risk:*** *The risk that security controls will not respond quickly and correctly to detect or prevent a risk event.*

Residual risk is the risk that remains after risk management controls have been implemented.

29.

Under which of the following access control models are a user's permissions MOST closely tied to their job?

Role-based access control

Rule-based access control

Attribute-based access control

Mandatory access control

Correct answer: Role-based access control

Several access control models exist, including:

- ***Mandatory Access Control (MAC):*** *MAC centrally controls access to resources based on a combination of sensitivity labels and user clearances. The military Unclassified/Confidential/Secret/Top Secret model with compartments is an example of a MAC system.*
- ***Discretionary Access Control (DAC):*** *DAC uses the concepts of users and groups and allows users to define who can access their resources. DAC is commonly used by computers, such as Linux's support for granting read/write/execute permissions to the owner, group, members, and others.*
- ***Role-Based Access Control (RBAC):*** *Role-based access control assigns each user with a role and a set of associated permissions, which are used to determine if a request is valid. For example, a software developer may have access to certain systems and tools, while a software manager may have access to HR information that the developer cannot access.*
- ***Rule-Based Access Control (RBAC):*** *Rule-based access control uses access control lists (ACLs) and Boolean logic to determine if a request is valid. For example, rules may restrict the times during which a system can be accessed or the devices permitted to access sensitive data.*
- ***Attribute-Based Access Control (ABAC):*** *ABAC assigns attributes to a user's identity that are used to determine their access. For example, a developer may have a certain set of permissions on one system but a different set on another.*
- ***Resource-Based Access Control (RBAC):*** *Resource-based access control systems include the Impersonation and Delegation Model used by Kerberos and the Trusted Subsystem Model. Under the Impersonation and Delegation Model, one entity delegates its access and privileges to another, allowing the other entity to impersonate it to achieve some task. The Trusted Subsystem Model controls access based on a trusted device rather than a user's identity.*

30.

Which of the following is focused on avoiding components shared between processes with different privilege levels?

Least Common Mechanism

Separation of Duties

Component Reuse

Diversity of Defense

Correct answer: Least Common Mechanism

Some of the key security design principles include:

- ***Least Common Mechanism:*** *Least common mechanism states that different processes with different privilege levels should not use the same function or mechanism because it is more difficult to keep these paths separate. Instead, each process should have its own mechanism.*
- ***Separation of Duties:*** *Separation of duties or compartmentalization divides high-risk or critical processes across multiple roles. This reduces the probability that a malicious user could carry out the action or be tricked into doing so.*
- ***Component Reuse:*** *Don't reinvent the wheel. The use of secure, high-quality components rather than custom code can improve the efficiency and security of software and reduce the attack surface.*
- ***Diversity of Defense:*** *Software defenses should be diverse geographically, technically, etc. This reduces the probability that an event affecting one defense will impact all of them.*

31.

The Trusted Subsystem Model and Impersonation and Delegation Model are examples of which type of access control?

Resource-based access control

Discretionary access control

Attribute-based access control

Rule-based access control

Correct answer: Resource-based access control

Several access control models exist, including:

- ***Mandatory Access Control (MAC):*** *MAC centrally controls access to resources based on a combination of sensitivity labels and user clearances. The military Unclassified/Confidential/Secret/Top Secret model with compartments is an example of a MAC system.*
- ***Discretionary Access Control (DAC):*** *DAC uses the concepts of users and groups and allows users to define who can access their resources. DAC is commonly used by computers, such as Linux's support for granting read/write/execute permissions to the owner, group, members, and others.*
- ***Role-Based Access Control (RBAC):*** *Role-based access control assigns each user with a role and a set of associated permissions, which are used to determine if a request is valid. For example, a software developer may have access to certain systems and tools, while a software manager may have access to HR information that the developer cannot access.*
- ***Rule-Based Access Control (RBAC):*** *Rule-based access control uses access control lists (ACLs) and Boolean logic to determine if a request is valid. For example, rules may restrict the times during which a system can be accessed or the devices permitted to access sensitive data.*
- ***Attribute-Based Access Control (ABAC):*** *ABAC assigns attributes to a user's identity that are used to determine their access. For example, a developer may have a certain set of permissions on one system but a different set on another.*
- ***Resource-Based Access Control (RBAC):*** *Resource-based access control systems include the Impersonation and Delegation Model used by Kerberos and the Trusted Subsystem Model. Under the Impersonation and Delegation Model, one entity delegates its access and privileges to another, allowing the other entity to impersonate it to achieve some task. The Trusted Subsystem Model controls access based on a trusted device rather than a user's identity.*

32.

The terms Constrained Data Items, Integrity Verification Processes, and Transformation Processes relate to which of the following?

Clark-Wilson

Bell-LaPadula

Biba

Brewer-Nash

Correct answer: Clark-Wilson

Clark-Wilson is a transaction-based integrity model that defines Constrained Data Items (CDIs) and Unconstrained Data Items (UDIs). Integrity Verification Processes (IVPs) verify that CDI meets integrity rules for a particular state, and Transformation Processes (TPs) can change CDIs from one valid state to another.

*Bell-LaPadula is a confidentiality protection model that combines attributes of Mandatory Access Control (MAC) and Discretionary Access Control (DAC). Its Simple Security Rule prevents reading data at a higher level of classification, while its * property prevents writing data to a system with a lower classification level.*

Biba is an integrity model designed to protect higher-level, more trustworthy data from being corrupted by lower-level data. Its no-write-up rule blocks systems from writing data to a system with a higher classification level. Its second rule states that a system reading/processing data from a lower-level system will have its integrity level lowered as a result.

Brewer-Nash or the Chinese Wall is a confidentiality model for enterprises. It addresses the case where one group within an organization may have information that cannot be shared with another.

33.

A user with a verified identity has gained access to systems that they should not be able to access. This is a failure of which of the following?

Authorization

Authentication

Accountability

Availability

Correct answer: Authorization

Authorization: *Validating that an authenticated user has the right to perform a particular action. Authorization can be managed via various access control models.*

Authentication: *Verifying the identity of the user. Common authentication factors include something you know (passwords, etc.), something you have (smartphone, etc.), and something you are (biometrics).*

Accountability: *Monitoring and recording activity by users on systems. Audit logs should include at a minimum the user's identity, the action taken, the object acted upon, and the time at which the action was taken.*

Availability: *Ensuring that authorized personnel can access systems or data. Load balancing, backups, and redundant systems are examples of solutions for protecting availability.*

34.

Which of the following is focused on planning to reduce software security risks in the future?

Bug tracking

Threat modeling

Fuzzing

Security review

Correct answer: Bug tracking

Bug tracking is the process of recording known issues with software to be fixed in the future.

Threat modeling identifies and describes potential threats to software, enabling mitigations to be implemented. Fuzzing automatically sends random and invalid inputs to a system to identify issues that could cause the program to crash or exhibit other undesirable behavior. Security reviews are periodic audits to validate that security processes are being properly performed during the software development lifecycle (SDLC).

35.

Which of the following confidentiality-preserving models combines aspects of MAC and DAC access control systems?

Bell-LaPadula

Biba

Clark-Wilson

Brewer-Nash

Correct answer: Bell-LaPadula

*Bell-LaPadula is a confidentiality protection model that combines attributes of Mandatory Access Control (MAC) and Discretionary Access Control (DAC). Its Simple Security Rule prevents reading data at a higher level of classification, while its * property prevents writing data to a system with a lower classification level.*

Biba is an integrity model designed to protect higher-level, more trustworthy data from being corrupted by lower-level data. Its no-write-up rule blocks systems from writing data to a system with a higher classification level. Its second rule states that a system reading/processing data from a lower-level system will have its integrity level lowered as a result.

Clark-Wilson is a transaction-based integrity model that defines Constrained Data Items (CDIs) and Unconstrained Data Items (UDIs). Integrity Verification Processes (IVPs) verify that CDI meets integrity rules for a particular state, and Transformation Processes (TPs) can change CDIs from one valid state to another.

Brewer-Nash or the Chinese Wall is a confidentiality model for enterprises. It addresses the case where one group within an organization may have information that cannot be shared with another.

36.

Which of the following models has a * property that prevents writing data to a system at a lower level?

Bell-LaPadula

Biba

Clark-Wilson

Brewer-Nash

Correct answer: Bell-LaPadula

*Bell-LaPadula is a confidentiality protection model that combines attributes of Mandatory Access Control (MAC) and Discretionary Access Control (DAC). Its Simple Security Rule prevents reading data at a higher level of classification, while its * property prevents writing data to a system with a lower classification level.*

Biba is an integrity model designed to protect higher-level, more trustworthy data from being corrupted by lower-level data. Its no-write-up rule blocks systems from writing data to a system with a higher classification level. Its second rule states that a system reading/processing data from a lower-level system will have its integrity level lowered as a result.

Clark-Wilson is a transaction-based integrity model that defines Constrained Data Items (CDIs) and Unconstrained Data Items (UDIs). Integrity Verification Processes (IVPs) verify that CDI meets integrity rules for a particular state, and Transformation Processes (TPs) can change CDIs from one valid state to another.

Brewer-Nash or the Chinese Wall is a confidentiality model for enterprises. It addresses the case where one group within an organization may have information that cannot be shared with another.

37.

Which of the following models is based on directed graphs?

Take-Grant

Biba

Clark-Wilson

Brewer-Nash

Correct answer: Take-Grant

The take-grant model is based on graph theory. A directed graph describes the relationships between nodes with each edge describing the take, grant, read, and write rights between nodes.

Biba is an integrity model designed to protect higher-level, more trustworthy data from being corrupted by lower-level data. Its no-write-up rule blocks systems from writing data to a system with a higher classification level. Its second rule states that a system reading/processing data from a lower-level system will have its integrity level lowered as a result.

Clark-Wilson is a transaction-based integrity model that defines Constrained Data Items (CDIs) and Unconstrained Data Items (UDIs). Integrity Verification Processes (IVPs) verify that CDI meets integrity rules for a particular state, and Transformation Processes (TPs) can change CDIs from one valid state to another.

Brewer-Nash or the Chinese Wall is a confidentiality model for enterprises. It addresses the case where one group within an organization may have information that cannot be shared with another.

38.

Shadow IT, when users implement non-approved solutions to problems, is MOST related to which of the following?

Psychological Acceptability

Component Reuse

Least Common Mechanism

Defense in Depth

Correct answer: Psychological Acceptability

Some of the key security design principles include:

- ***Psychological Acceptability:*** *If users don't understand a security control or feel that it obstructs their work, they'll attempt to work around it, undermining it. Security functionality should be user-friendly and transparent to the user.*
- ***Defense in Depth:*** *The principle of defense in depth states that assets should be protected by multiple independent layers of security. The use of layered security makes it more difficult for an attacker to bypass or defeat every defense and achieve their objective.*
- ***Least Common Mechanism:*** *Least common mechanism states that different processes with different privilege levels should not use the same function or mechanism because it is more difficult to keep these paths separate. Instead, each process should have its own mechanism.*
- ***Component Reuse:*** *Don't reinvent the wheel. The use of secure, high-quality components rather than custom code can improve the efficiency and security of software and reduce the attack surface.*

39.

Which of the following can help to protect against a user fraudulently performing high-risk actions on a system?

Separation of Duties

Economy of Mechanism

Complete Mediation

Diversity of Defense

Correct answer: Separation of Duties

Some of the key security design principles include:

- ***Separation of Duties:*** *Separation of duties or compartmentalization divides high-risk or critical processes across multiple roles. This reduces the probability that a malicious user could carry out the action or be tricked into doing so.*
- ***Economy of Mechanism:*** *Economy of Mechanism or "Keep It Simple" states that the design and implementation of software should be as simple as possible. Complex systems have a larger attack surface and are more difficult to troubleshoot if something goes wrong.*
- ***Complete Mediation:*** *Complete mediation states that authorization should be performed for every request, even if requests are repeated. This ensures that the authorization system is never bypassed.*
- ***Diversity of Defense:*** *Software defenses should be diverse geographically, technically, etc. This reduces the probability that an event affecting one defense will impact all of them.*

40.

Which of the following is focused on reducing the total attack surface of an application?

Leveraging existing components

Least common mechanism

Least privilege

Separation of duties

Correct answer: Leveraging existing components

Leveraging existing components encourages code reuse because it reduces an application's attack surface and the risk of new vulnerabilities being introduced into software.

Least common mechanism prevents against sharing mechanisms or functions in code that are used by different users or processes if they have different levels of privilege.

The principle of least privilege states that users, applications, etc. should only have the access and privileges needed to do their jobs.

Separation of duties refers to the fact that critical processes (such as approving payments) should be split across multiple people to protect against fraud, social engineering, etc.

41.

Which of the following is NOT one of the three main types of authentication factors?

Something you do

Something you know

Something you have

Something you are

Correct answer: Something you do

The three main types of authentication factors are:

- *Something you know (passwords, etc.)*
- *Something you have (smartphone, token, etc.)*
- *Something you are (biometrics, etc.)*

Behavioral factors such as "something you do" can be used for authentication, but this is not one of the main three types of authentication factors.

42.

A potential issue overlooked during an audit is an example of which of the following?

Detection risk

Inherent risk

Control risk

Residual risk

Correct answer: Detection risk

The three forms of audit-related risk are:

- ***Inherent Risk:*** *Risks that are inherent to a particular process or tool that should be managed by security controls.*
- ***Detection Risk:*** *The risk that a potential issue will be undetected by an audit, causing a potential issue.*
- ***Control Risk:*** *The risk that security controls will not respond quickly and correctly to detect or prevent a risk event.*

Residual risk is the risk that remains after risk management controls have been implemented.

43.

Which of the following is LEAST related to the others?

- **Availability**
- Authorization
- Accountability
- Authentication

Correct answer: Availability

Availability is not part of the AAA of authentication, authorization, and accountability, which have the following definitions:

- ***Authentication:*** *Verifying the identity of the user. Common authentication factors include something you know (passwords, etc.), something you have (smartphone, etc.), and something you are (biometrics).*
- ***Authorization:*** *Validating that an authenticated user has the right to perform a particular action. Authorization can be managed via various access control models.*
- ***Accountability:*** *Monitoring and recording activity by users on systems. Audit logs should include at a minimum the user's identity, the action taken, the object acted upon, and the time at which the action was taken.*

44.

Which of the following is NOT one of the foundational system tenets?

Threat management

Session management

Exception management

Configuration management

Correct answer: Threat management

The three foundational system tenets are:

- ***Session Management:*** *Management of communication sessions between multiple components*
- ***Exception Management:*** *Correct management of error conditions*
- ***Configuration Management:*** *Management of system configurations to ensure functionality and security*

45.

Which of the following is NOT true of OpenID?

It performs authorization

It verifies a user's identity

It does not require an existing RP-IdP relationship

It uses a universal identifier

Correct answer: It performs authorization

OpenID proves a user's identity and uses a universal identifier. It does not require a prearranged relationship between the Identity Provider (IdP) and the Relying Party (RP).
OAuth requires a prearranged relationship between an IdP and an RP and generates an access token for user authorization.

46.

The Linux access control model of assigning read, write, and execute privileges to a user, group, and others is an example of which access control model?

DAC

MAC

RBAC

ABAC

Correct answer: DAC

Several access control models exist, including:

- ***Mandatory Access Control (MAC):*** *MAC centrally controls access to resources based on a combination of sensitivity labels and user clearances. The military Unclassified/Confidential/Secret/Top Secret model with compartments is an example of a MAC system.*
- ***Discretionary Access Control (DAC):*** *DAC uses the concepts of users and groups and allows users to define who can access their resources. DAC is commonly used by computers, such as Linux's support for granting read/write/execute permissions to the owner, group, members, and others.*
- ***Role-Based Access Control (RBAC):*** *Role-based access control assigns each user with a role and a set of associated permissions, which are used to determine if a request is valid. For example, a software developer may have access to certain systems and tools, while a software manager may have access to HR information that the developer cannot access.*
- ***Rule-Based Access Control (RBAC):*** *Rule-based access control uses access control lists (ACLs) and Boolean logic to determine if a request is valid. For example, rules may restrict the times during which a system can be accessed or the devices permitted to access sensitive data.*
- ***Attribute-Based Access Control (ABAC):*** *ABAC assigns attributes to a user's identity that are used to determine their access. For example, a developer may have a certain set of permissions on one system but a different set on another.*
- ***Resource-Based Access Control (RBAC):*** *Resource-based access control systems include the Impersonation and Delegation Model used by Kerberos and the Trusted Subsystem Model. Under the Impersonation and Delegation Model, one entity delegates its access and privileges to another, allowing the other entity to impersonate it to achieve some task. The Trusted Subsystem Model controls access based on a trusted device rather than a user's identity.*

47.

Which of the following is intended to identify errors or vulnerabilities in a program's code?

Fuzzing

Bug tracking

Threat modeling

Security review

Correct answer: Fuzzing

Fuzzing automatically sends random and invalid inputs to a system to identify issues that could cause the program to crash or exhibit other undesirable behavior.

Bug tracking is the process of recording known issues with software to be fixed in the future. Threat modeling identifies and describes potential threats to software, enabling mitigations to be implemented. Security reviews are periodic audits to validate that security processes are being properly performed during the software development lifecycle (SDLC).

48.

Which of the following is designed to ensure that security processes are being followed?

Security review

Bug tracking

Fuzzing

Threat modeling

Correct answer: Security review

Security reviews are periodic audits to validate that security processes are being properly performed during the software development lifecycle (SDLC).

Bug tracking is the process of recording known issues with software to be fixed in the future. Threat modeling identifies and describes potential threats to software, enabling mitigations to be implemented. Fuzzing automatically sends random and invalid inputs to a system to identify issues that could cause the program to crash or exhibit other undesirable behavior.

49.

Which of the following is NOT one of the three primary means of managing security risks in production systems?

- **Avoidance**
- Prevention
- Detection
- Response

Correct answer: Avoidance

The three main methods of managing security risks in production systems are prevention, detection, and response.

50.

Which of the following access control models assigns tags to users' identities for use in access determinations?

ABAC

MAC

RBAC

DAC

Correct answer: ABAC

Several access control models exist, including:

- ***Mandatory Access Control (MAC):*** *MAC centrally controls access to resources based on a combination of sensitivity labels and user clearances. The military Unclassified/Confidential/Secret/Top Secret model with compartments is an example of a MAC system.*
- ***Discretionary Access Control (DAC):*** *DAC uses the concepts of users and groups and allows users to define who can access their resources. DAC is commonly used by computers, such as Linux's support for granting read/write/execute permissions to the owner, group, members, and others.*
- ***Role-Based Access Control (RBAC):*** *Role-based access control assigns each user with a role and a set of associated permissions, which are used to determine if a request is valid. For example, a software developer may have access to certain systems and tools, while a software manager may have access to HR information that the developer cannot access.*
- ***Rule-Based Access Control (RBAC):*** *Rule-based access control uses access control lists (ACLs) and Boolean logic to determine if a request is valid. For example, rules may restrict the times during which a system can be accessed or the devices permitted to access sensitive data.*
- ***Attribute-Based Access Control (ABAC):*** *ABAC assigns attributes to a user's identity that are used to determine their access. For example, a developer may have a certain set of permissions on one system but a different set on another.*
- ***Resource-Based Access Control (RBAC):*** *Resource-based access control systems include the Impersonation and Delegation Model used by Kerberos and the Trusted Subsystem Model. Under the Impersonation and Delegation Model, one entity delegates its access and privileges to another, allowing the other entity to impersonate it to achieve some task. The Trusted Subsystem Model controls access based on a trusted device rather than a user's identity.*

51.

Which of the following is a planning tool designed to ensure that software addresses all potential threats?

Threat modeling

Bug tracking

Fuzzing

Security review

Correct answer: Threat modeling

Threat modeling identifies and describes potential threats to software, enabling mitigations to be implemented.

Bug tracking is the process of recording known issues with software to be fixed in the future. Fuzzing automatically sends random and invalid inputs to a system to identify issues that could cause the program to crash or exhibit other undesirable behavior. Security reviews are periodic audits to validate that security processes are being properly performed during the software development lifecycle (SDLC).

52.

Which of the following is also known as the "Keep It Simple" principle?

- **Economy of mechanism**
- Least common mechanism
- Psychological acceptability
- Open design

Correct answer: Economy of mechanism

Economy of mechanism (also known as the Keep it Simple principle) states that software design and implementation should be as simple as possible to reduce the risk of errors.

Open design is the opposite of security by obscurity and states that the security of software shouldn't depend on its design remaining secret.

Psychological acceptability indicates that users are more likely to comply with security requirements that are easy to use and transparent.

Least common mechanism prevents against sharing mechanisms or functions in code that are used by different users or processes if they have different levels of privilege.

53.

Which of the following acronyms is shared by multiple access control models?

RBAC

MAC

DAC

ABAC

Correct answer: RBAC

Several access control models exist, including:

- ***Mandatory Access Control (MAC):*** *MAC centrally controls access to resources based on a combination of sensitivity labels and user clearances. The military Unclassified/Confidential/Secret/Top Secret model with compartments is an example of a MAC system.*
- ***Discretionary Access Control (DAC):*** *DAC uses the concepts of users and groups and allows users to define who can access their resources. DAC is commonly used by computers, such as Linux's support for granting read/write/execute permissions to the owner, group, members, and others.*
- ***Role-Based Access Control (RBAC):*** *Role-based access control assigns each user with a role and a set of associated permissions, which are used to determine if a request is valid. For example, a software developer may have access to certain systems and tools, while a software manager may have access to HR information that the developer cannot access.*
- ***Rule-Based Access Control (RBAC):*** *Rule-based access control uses access control lists (ACLs) and Boolean logic to determine if a request is valid. For example, rules may restrict the times during which a system can be accessed or the devices permitted to access sensitive data.*
- ***Attribute-Based Access Control (ABAC):*** *ABAC assigns attributes to a user's identity that are used to determine their access. For example, a developer may have a certain set of permissions on one system but a different set on another.*
- ***Resource-Based Access Control (RBAC):*** *Resource-based access control systems include the Impersonation and Delegation Model used by Kerberos and the Trusted Subsystem Model. Under the Impersonation and Delegation Model, one entity delegates its access and privileges to another, allowing the other entity to impersonate it to achieve some task. The Trusted Subsystem Model controls access based on a trusted device rather than a user's identity.*

54.

Which type of risk are security controls primarily focused on managing?

Inherent risk

Detection risk

Control risk

Residual risk

Correct answer: Inherent risk

The three forms of audit-related risk are:

- ***Inherent Risk:*** *Risks that are inherent to a particular process or tool that should be managed by security controls.*
- ***Detection Risk:*** *The risk that a potential issue will be undetected by an audit, causing a potential issue.*
- ***Control Risk:*** *The risk that security controls will not respond quickly and correctly to detect or prevent a risk event.*

Residual risk is the risk that remains after risk management controls have been implemented.

55.

Which of the following is a model focused on protecting data from unauthorized modification?

- **Biba**
- Bell-LaPadula
- Take-Grant
- Brewer-Nash

Correct answer: Biba

Biba is an integrity model designed to protect higher-level, more trustworthy data from being corrupted by lower-level data. Its no-write-up rule blocks systems from writing data to a system with a higher classification level. Its second rule states that a system reading/processing data from a lower-level system will have its integrity level lowered as a result.

*Bell-LaPadula is a confidentiality protection model that combines attributes of Mandatory Access Control (MAC) and Discretionary Access Control (DAC). Its Simple Security Rule prevents reading data at a higher level of classification, while its * property prevents writing data to a system with a lower classification level.*

The take-grant model is based on graph theory. A directed graph describes the relationships between nodes with each edge describing the take, grant, read, and write rights between nodes.

Brewer-Nash or the Chinese Wall is a confidentiality model for enterprises. It addresses the case where one group within an organization may have information that cannot be shared with another.

56.

Which of the following is the OPPOSITE of security by obscurity?

Open design

Psychological acceptability

Defense in depth

Fail secure

Correct answer: Open design

Open design is the opposite of security by obscurity and states that the security of software shouldn't depend on its design remaining secret.

Psychological acceptability indicates that users are more likely to comply with security requirements that are easy to use and transparent.

Defense in depth means that multiple layers of security should be used so that a failure of one layer doesn't leave the system vulnerable.

Fail secure means that a system should default to a secure state if something goes wrong, rather than an insecure one. For example, magnetic locks on a secure area should be locked if they lose power.

57.

Which of the following focuses on protecting data from unauthorized modification?

Integrity

Confidentiality

Availability

Non-Repudiation

Correct answer: Integrity

Some of the core goals of cryptographic algorithms include:

- ***Confidentiality:*** *Protecting sensitive information from being disclosed to unauthorized parties. Confidentiality can be protected overtly (encryption, hashing) or covertly (steganography, digital watermarking).*
- ***Integrity:*** *Preventing data from being modified without authorization. Data integrity can be protected by hash functions, digital signatures, parity bits, and cyclic redundancy checking.*
- ***Availability:*** *Ensuring that authorized personnel can access systems or data. Load balancing, backups, and redundant systems are examples of solutions for protecting availability.*
- ***Non-Repudiation:*** *Preventing a user from denying that they took a particular action. Digital signatures and the blockchain's immutable ledger are examples of protections against repudiation.*

58.

Implementing defense in depth can help to protect against which of the following?

Control risk

Inherent risk

Detection risk

Residual risk

Correct answer: Control risk

The three forms of audit-related risk are:

- ***Inherent Risk:*** *Risks that are inherent to a particular process or tool that should be managed by security controls.*
- ***Detection Risk:*** *The risk that a potential issue will be undetected by an audit, causing a potential issue.*
- ***Control Risk:*** *The risk that security controls will not respond quickly and correctly to detect or prevent a risk event.*

Defense in depth refers to the use of layered security controls to ensure that, if one fails, another manages the issue. Therefore, it can help to manage control risks, which refer to the risk that a security control will fail to detect or prevent a risk event.

Residual risk is the risk that remains after risk management controls have been implemented.

59.

Which of the following is the LAST stage in managing security risks in production systems?

Response

Prevention

Detection

Proactive security

Correct answer: Response

The three main ways to manage security risks in production include:

- ***Prevention:** Blocking a security incident from occurring. Examples of preventative controls include firewalls, access controls, and encryption.*
- ***Detection:** Identifying a security incident that requires mitigation. Detective controls include audit logs, honeypots, and intrusion detection systems (IDS).*
- ***Response:** Mitigating an identified security incident. Incident response efforts are supported by backups, incident response teams (IRTs), and computer forensics.*

Prevention should come first, followed by detection and response if prevention fails.

Proactive security actions would involve threat hunting or similar activities.

60.

Which of the following focuses on protecting sensitive information from unauthorized access?

- **Confidentiality**
- Integrity
- Availability
- Non-Repudiation

Correct answer: Confidentiality

Some of the core goals of cryptographic algorithms include:

- ***Confidentiality:*** *Protecting sensitive information from being disclosed to unauthorized parties. Confidentiality can be protected overtly (encryption, hashing) or covertly (steganography, digital watermarking).*
- ***Integrity:*** *Preventing data from being modified without authorization. Data integrity can be protected by hash functions, digital signatures, parity bits, and cyclic redundancy checking.*
- ***Availability:*** *Ensuring that authorized personnel can access systems or data. Load balancing, backups, and redundant systems are examples of solutions for protecting availability.*
- ***Non-Repudiation:*** *Preventing a user from denying that they took a particular action. Digital signatures and the blockchain's immutable ledger are examples of protections against repudiation.*

Domain 2: Secure Software Lifecycle Management

61.

Risk to software itself is classified as which of the following?

- **Technical risk**
- Business risk
- Exploitation risk
- Inherent risk

Correct answer: Technical risk

Technical risk is the risk posed by threats to software by attacks against it.

Business risk is the risk posed to the business by attacks against software and the resulting loss of functionality.

62.

Which of the following security metrics could BEST be used to measure the success of an OWASP-focused developer training program?

Number of common errors

Defects per thousand lines of code

Number of repeated errors

Average time to remediate an issue

Correct answer: Number of common errors

Metrics for measuring security can include:

- *Defects per thousand lines of code*
- *Number of repeated errors*
- *Number of common errors*
- *Percent of errors above a criticality level*
- *Average time to remediate an issue*
- *Complexity associated with errors*

63.

Which of the following security controls is MOST related to compliance?

Compensating

Corrective

Detective

Deterrent

Correct answer: Compensating

The five types of security controls are:

- ***Detective:*** *Build a log of system or user actions that can be used to identify anomalies and potential threats.*
- ***Preventative:*** *Actively or proactively work to block an attack.*
- ***Deterrent:*** *Attempt to dissuade an attacker from carrying out an attack.*
- ***Corrective:*** *Help to recover back to normal operations after an attack.*
- ***Compensating:*** *Provide an alternative to a security requirement when the recommended control cannot be implemented for some reason.*

64.

Which of the following development methodologies is MOST people-centric?

XP

Scrum

Waterfall

Spiral

Correct answer: XP

XP is a people-centric approach to development that iteratively storyboards and implements user requirements.

Scrum is an Agile development method in which participants are classified as pigs or chickens and have defined roles in project development. Development is broken into sprints designed to implement specific features.

Waterfall is a predictive development methodology with a linear, sequential process through stages with no backtracking. In Waterfall, identifying issues early is critical, as it is difficult to fix problems after the face.

The Spiral model combines elements of Waterfall and prototyping models. It incorporates risk assessments at each of its phases, enabling a team to minimize sunk costs on a failed project.

65.

Which of the following risk management techniques reduces the total amount of risk?

Mitigation

Acceptance

Transference

Avoidance

Correct answer: Mitigation

Organizations have a few options when dealing with risk, including:

- ***Mitigation:*** *Take steps to reduce or eliminate the risk*
- ***Acceptance:*** *Accept the potential risk and do nothing*
- ***Transference:*** *Pass the risk on to an insurer, user, or other party*
- ***Avoidance:*** *Stop performing the risky activity*

66.

An access control list (ACL) falls under which category of security control?

Technical

Administrative

Physical

Logical

Correct answer: Technical

Security controls can be classified into three classes:

- ***Administrative:*** *Administrative controls are guidelines, policies, and procedures. For example, many companies have a security policy that details acceptable use of their systems.*
- ***Technical:*** *Technical security controls use software to protect against threats. Access control lists (ACLs) are an example of a technical control.*
- ***Physical:*** *Physical controls are designed to provide physical security. Photo IDs, motion detectors, and security cameras are examples of physical controls.*

Logical is not a type of security control.

67.

A "use at your own risk" banner is an example of which risk management strategy?

- **Transference**
- Mitigation
- Acceptance
- Avoidance

Correct answer: Transference

Organizations have a few options when dealing with risk, including:

- ***Mitigation:*** *Take steps to reduce or eliminate the risk*
- ***Acceptance:*** *Accept the potential risk and do nothing*
- ***Transference:*** *Pass the risk on to an insurer, user, or other party*
- ***Avoidance:*** *Stop performing the risky activity*

68.

The risk that attacks against software may deprive the organization of the software's capabilities is classified as which of the following?

Business risk

Technical risk

Operational risk

Opportunity risk

Correct answer: Business risk

Technical risk is the risk posed by threats to software by attacks against it. Business risk is the risk posed to the business by attacks against software and the resulting loss of functionality.

69.

What is the term for a feature that can be exploited by an attacker?

Vulnerability

Threat

Flaw

Bug

Correct answer: Vulnerability

A vulnerability is any feature of an asset that can be exploited by an attacker for a malicious purpose.

A threat is anything that can cause harm to an organization and its assets.

Flaws and bugs may be vulnerabilities, but they may also not be exploitable

70.

Which of the following estimates the number of times that an organization will face a particular threat?

ARO

SLE

ALE

SRO

Correct answer: ARO

Annual Rate of Occurrence (ARO) estimates the number of times that a specific threat will materialize each year.

Single Loss Expectancy (SLE) estimates the loss caused by a threat and is calculated as the product of the asset value and the exposure factor.

Annual Loss Expectancy (ALE) estimates the loss caused by a threat across an entire year. It is calculated as the product of SLO and ARO.

71.

Which of the following is an OWASP-developed resource for improving the security of the software development process?

SAMM

BSIMM

FIPS

SAFECode

Correct answer: SAMM

Some useful resources for software security information include:

- ***National Institute of Standards and Technology (NIST):*** *NIST publishes various standards, including Special Publications (SPs) and Federal Information Processing Standards (FIPS).*
- ***Software Assurance Forum for Excellence in Code (SAFECode):*** *SAFECode offers a collaboration environment for organizations to discuss software security best practices.*
- ***Software Assurance Maturity Model (SAMM):*** *SAMM is a framework developed by OWASP to improve the security of the software development process.*
- ***Building Security in Maturity Model (BSIMM):*** *BSIMM quantifies the maturity and effectiveness of an organization's application security (AppSec) program.*

72.

What is the term for something put in place to manage the risk posed by a threat and that is classified as preventative, detective, corrective, or compensating?

Control

Mitigation

Defense

Protection

Correct answer: Control

Controls are measures put in place to detect, prevent, or mitigate the risks posed by a threat.

73.

Which of the following incorporates risk assessments in each phase of the project, allowing developers to cut their losses?

Spiral

Scrum

XP

Waterfall

Correct answer: Spiral

Scrum is an Agile development method in which participants are classified as pigs or chickens and have defined roles in project development. Development is broken into sprints designed to implement specific features.

XP is a people-centric approach to development that iteratively storyboards and implements user requirements.

Waterfall is a predictive development methodology with a linear, sequential process through stages with no backtracking. In Waterfall, identifying issues early is critical, as it is difficult to fix problems after the fact.

The Spiral model combines elements of Waterfall and prototyping models. It incorporates risk assessments at each of its phases, enabling a team to minimize sunk costs on a failed project.

74.

Which of the following manages how hardware, software, documentation, interfaces, and patching are set up?

Configuration control

Version control

Revision control

Baseline control

Correct answer: Configuration control

Configuration control manages the configuration of hardware, software, documentation, interfaces, and patching.

Version control involves managing the versions and changes to files and a codebase. Revision control is related to version control and involves defining and labeling each release. Baseline control is part of configuration management and includes change accounting and library management.

75.

Which of the following can quantify the cost that an attack has to an organization?

SLE

ARO

ALE

SRO

Correct answer: SLE

Single Loss Expectancy (SLE) estimates the loss caused by a threat and is calculated as the product of the asset value and the exposure factor.

Annual Rate of Occurrence (ARO) estimates the number of times that a specific threat will materialize each year.

Annual Loss Expectancy (ALE) estimates the loss caused by a threat across an entire year. It is calculated as the product of SLO and ARO.

76.

Which of the following focuses on offering a platform for organizations to collaborate and discuss security best practices?

SAFECode

NIST

ISO

BSIMM

Correct answer: SAFECode

Some useful resources for software security information include:

- ***International Organization for Standardization (ISO):*** *ISO publishes a variety of different standards, including some that address software security.*
- ***National Institute of Standards and Technology (NIST):*** *NIST publishes various standards, including Special Publications (SPs) and Federal Information Processing Standards (FIPS).*
- ***Software Assurance Forum for Excellence in Code (SAFECode):*** *SAFECode offers a collaboration environment for organizations to discuss software security best practices.*
- ***Building Security in Maturity Model (BSIMM):*** *BSIMM quantifies the maturity and effectiveness of an organization's application security (AppSec) program.*

77.

Which type of control actively works against the attacker?

- **Preventative**
- Deterrent
- Compensating
- Corrective

Correct answer: Preventative

The five types of security controls are:

- ***Detective:*** *Build a log of system or user actions that can be used to identify anomalies and potential threats.*
- ***Preventative:*** *Actively or proactively work to block an attack.*
- ***Deterrent:*** *Attempt to dissuade an attacker from carrying out an attack.*
- ***Corrective:*** *Help to recover back to normal operations after an attack.*
- ***Compensating:*** *Provide an alternative to a security requirement when the recommended control cannot be implemented for some reason.*

78.

Defining and labeling each code release is part of which of the following?

Revision control

Configuration control

Version control

Baseline control

Correct answer: Revision control

Revision control is related to version control and involves defining and labeling each release.

Configuration control manages the configuration of hardware, software, documentation, interfaces, and patching. Version control involves managing the versions and changes to files and a codebase. Baseline control is part of configuration management and includes change accounting and library management.

79.

Which of the following risk mitigation strategies requires the GREATEST risk appetite?

Acceptance

Mitigation

Transference

Avoidance

Correct answer: Acceptance

Organizations have a few options when dealing with risk, including:

- ***Mitigation:*** *Take steps to reduce or eliminate the risk*
- ***Acceptance:*** *Accept the potential risk and do nothing*
- ***Transference:*** *Pass the risk on to an insurer, user, or other party*
- ***Avoidance:*** *Stop performing the risky activity*

Risk appetite measures the amount of risk that an organization is willing to accept.

80.

Which of the following is NOT a main component of configuration management?

Revision control

Change process management

Baseline control

Configuration verification

Correct answer: Revision control

Configuration management is composed of configuration control and verification control. Three main components of this are:

- *Change process management (change authorization, verification control, and release processing)*
- *Baseline control (change accounting and library management)*
- *Configuration verification (status accounting for compliance with specifications)*

81.

Which of the following types of security controls is focused on restoring normal operations after an attack?

Corrective

Compensating

Deterrent

Preventative

Correct answer: Corrective

The five types of security controls are:

- ***Detective:*** *Build a log of system or user actions that can be used to identify anomalies and potential threats.*
- ***Preventative:*** *Actively or proactively work to block an attack.*
- ***Deterrent:*** *Attempt to dissuade an attacker from carrying out an attack.*
- ***Corrective:*** *Help to recover back to normal operations after an attack.*
- ***Compensating:*** *Provide an alternative to a security requirement when the recommended control cannot be implemented for some reason.*

82.

Which of the following roles is responsible for maintenance of a system after release?

Customer

Supplier

Configuration manager

Subcontractor

Correct answer: Customer

The customer role is responsible for post-release maintenance of a system.

The supplier role is responsible for pre-release product configuration. Configuration managers ensure that the configuration plan is followed throughout the development process.

83.

Changes to an organization's codebase should be managed by which of the following?

Version control

Configuration control

Revision control

Baseline control

Correct answer: Version control

Version control involves managing the versions and changes to files and a codebase.

Revision control is related to version control and involves defining and labeling each release. Configuration control manages the configuration of hardware, software, documentation, interfaces, and patching. Baseline control is part of configuration management and includes change accounting and library management.

84.

Which of the following is NOT one of the three classes of security controls?

Procedural

Administrative

Technical

Physical

Correct answer: Procedural

Security controls can be classified into three classes:

- *Administrative*
- *Technical*
- *Physical*

85.

Which of the following organizations publishes internationally accepted best practices and standards in various areas?

ISO

OWASP

PCI

NIST

Correct answer: ISO

Some useful resources for software security information include:

- ***International Organization for Standardization (ISO):*** *ISO publishes a variety of different standards, including some that address software security.*
- ***Payment Card Industry (PCI):*** *PCI-DSS is a data security standard focused on protecting the sensitive data of payment card holders and preventing payment card fraud.*
- ***National Institute of Standards and Technology (NIST):*** *NIST publishes various standards, including Special Publications (SPs) and Federal Information Processing Standards (FIPS).*
- ***Open Web Application Security Project (OWASP):*** *OWASP maintains several top ten vulnerability lists for various types of software and creates a range of security resources.*

86.

What is the term for risk that an organization MUST accept?

- **Residual risk**
- Mandatory risk
- Accepted risk
- Unavoidable risk

Correct answer: Residual risk

Residual risk is the risk that is left over after risk mitigation actions have occurred that an organization must accept.

87.

The probability of an attack does NOT measure which of the following?

- **Impact**
- Exploitability
- Discoverability
- Reproducibility

Correct answer: Impact

The probability of an attack measures how likely it is that an attacker will discover a vulnerability, develop an attack, and successfully exploit the vulnerability.

Impact measures the loss when an attacker exploits a vulnerability.

88.

Which of the following estimates the cost of a threat to the organization each year?

ALE

SLE

ARO

SRO

Correct answer: ALE

Annual Loss Expectancy (ALE) estimates the loss caused by a threat across an entire year. It is calculated as the product of SLO and ARO.

Single Loss Expectancy (SLE) estimates the loss caused by a threat and is calculated as the product of the asset value and the exposure factor.

Annual Rate of Occurrence (ARO) estimates the number of times that a specific threat will materialize each year.

89.

What is the term for a framework for containing policies, procedures, and technologies to manage various risks throughout the enterprise?

Integrated Risk Management

Holistic Risk Management

Governance, Risk, and Compliance

Centralized Risk Management

Correct answer: Integrated Risk Management

Integrated risk management (IRM) is a framework for policies, procedures, and technologies to manage various risks throughout the enterprise.

90.

Which of the following produces recommendations in the form of Special Publications?

NIST

ISO

OWASP

PCI

Correct answer: NIST

Some useful resources for software security information include:

- ***International Organization for Standardization (ISO):*** *ISO publishes a variety of different standards, including some that address software security.*
- ***Payment Card Industry (PCI):*** *PCI-DSS is a data security standard focused on protecting the sensitive data of payment card holders and preventing payment card fraud.*
- ***National Institute of Standards and Technology (NIST):*** *NIST publishes various standards, including Special Publications (SPs) and Federal Information Processing Standards (FIPS).*
- ***Open Web Application Security Project (OWASP):*** *OWASP maintains several top ten vulnerability lists for various types of software and creates a range of security resources.*

91.

Which of the following security metrics is the MOST widely used?

Defects per thousand lines of code

Number of repeated errors

Percent of errors above a criticality level

Average time to remediate an issue

Correct answer: Defects per thousand lines of code

Metrics for measuring security can include:

- *Defects per thousand lines of code*
- *Number of repeated errors*
- *Number of common errors*
- *Percent of errors above a criticality level*
- *Average time to remediate an issue*
- *Complexity associated with errors*

92.

Which of the following software end-of-life activities may be necessary to comply with regulatory compliance requirements for data retention?

Archiving

Credential Removal

Configuration Removal

License Cancellation

Correct answer: Archiving

End-of-life policies should include:

- ***Credential Removal:*** *Cancelling accounts, credentials, and permissions associated with the software*
- ***Configuration Removal:*** *Updating firewall rules and other configuration settings designed to allow the software to operate*
- ***License Cancellation:*** *Cancelling any license subscriptions that were needed to run the software*
- ***Archiving:*** *Maintaining a copy of the software and associated documentation in case it is needed in the future or for regulatory compliance*

93.

Pig and chicken roles are part of which development method?

Scrum

XP

Waterfall

Spiral

Correct answer: Scrum

Scrum is an Agile development method in which participants are classified as pigs or chickens and have defined roles in project development. Development is broken into sprints designed to implement specific features.

XP is a people-centric approach to development that iteratively storyboards and implements user requirements.

Waterfall is a predictive development methodology with a linear, sequential process through stages with no backtracking. In Waterfall, identifying issues early is critical, as it is difficult to fix problems after the fact.

The Spiral model combines elements of Waterfall and prototyping models. It incorporates risk assessments at each of its phases, enabling a team to minimize sunk costs on a failed project.

94.

Which of the following security metrics can measure a development team's ability to retain institutional knowledge?

Number of repeated errors

Number of common errors

Percent of errors above a criticality level

Complexity associated with errors

Correct answer: Number of repeated errors

Metrics for measuring security can include:

- *Defects per thousand lines of code*
- *Number of repeated errors*
- *Number of common errors*
- *Percent of errors above a criticality level*
- *Average time to remediate an issue*
- *Complexity associated with errors*

95.

Which type of control is focused on logging activities on a system?

Detective

Deterrent

Corrective

Compensating

Correct answer: Detective

The five types of security controls are:

- ***Detective:*** *Build a log of system or user actions that can be used to identify anomalies and potential threats.*
- ***Preventative:*** *Actively or proactively work to block an attack*
- ***Deterrent:*** *Attempt to dissuade an attacker from carrying out an attack.*
- ***Corrective:*** *Help to recover back to normal operations after an attack.*
- ***Compensating:*** *Provide an alternative to a security requirement when the recommended control cannot be implemented for some reason.*

96.

The corporate security policy falls into which class of security controls?

Administrative

Technical

Physical

Procedural

Correct answer: Administrative

Security controls can be classified into three classes:

- ***Administrative:*** *Administrative controls are guidelines, policies, and procedures. For example, many companies have a security policy that details acceptable use of their systems.*
- ***Technical:*** *Technical security controls use software to protect against threats. Access control lists (ACLs) are an example of a technical control.*
- ***Physical:*** *Physical controls are designed to provide physical security. Photo IDs, motion detectors, and security cameras are examples of physical controls.*

Procedural is not a type of security control.

97.

Which of the following terms is commonly used to describe adherence to external rules and laws?

Compliance

Conformance

Cooperation

Concession

Correct answer: Compliance

Compliance refers to an organization's adherence to external regulations and laws.

Conformance deals with adherence to internal requirements, such as organizational standards and policies.

98.

Which of the following is NOT part of change process management?

Change accounting

Change authorization

Verification control

Release processing

Correct answer: Change accounting

Configuration management is composed of configuration control and verification control. Three main components of this are:

- *Change process management (change authorization, verification control, and release processing)*
- *Baseline control (change accounting and library management)*
- *Configuration verification (status accounting for compliance with specifications)*

99.

In which of the following is identifying oversights, such as missing requirements, early the MOST critical?

Waterfall

Scrum

XP

Spiral

Correct answer: Waterfall

Waterfall is a predictive development methodology with a linear, sequential process through stages with no backtracking. In Waterfall, identifying issues early is critical, as it is difficult to fix problems after the fact.

Scrum is an Agile development method in which participants are classified as pigs or chickens and have defined roles in project development. Development is broken into sprints designed to implement specific features.

XP is a people-centric approach to development that iteratively storyboards and implements user requirements.

The Spiral model combines elements of Waterfall and prototyping models. It incorporates risk assessments at each of its phases, enabling a team to minimize sunk costs on a failed project.