Number: CCZT
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: CCZT

Exam Name: Certificate Of Competence In Zero Trust

Exam A

QUESTION 1
Of the following options, which risk/threat does SDP mitigate by mandating micro-segmentation and implementing least privilege?

A. Identification and authentication failures
B. Injection
C. Security logging and monitoring failures
D. Broken access control

Correct Answer: D
Section:
Explanation:
SDP mitigates the risk of broken access control by mandating micro-segmentation and implementing least privilege. Micro-segmentation divides the network into smaller, isolated segments that can prevent unauthorized access and contain lateral movement. Least privilege grants the minimum necessary access to users and devices for specific resources, while hiding all other assets from their view. This reduces the attack surface and prevents attackers from exploiting weak or misconfigured access controls

QUESTION 2
What should an organization's data and asset classification be based on?

A. Location of data
B. History of data
C. Sensitivity of data
D. Recovery of data

Correct Answer: C
Section:
Explanation:
Data and asset classification should be based on the sensitivity of data, which is the degree to which the data requires protection from unauthorized access, modification, or disclosure. Data sensitivity is determined by the potential impact of data loss, theft, or corruption on the organization, its customers, and its partners. Data sensitivity can also be influenced by legal, regulatory, and contractual obligations.
Reference =
Certificate of Competence in Zero Trust (CCZT) prepkit, page 10, section 2.1.1
Identify and protect sensitive business data with Zero Trust, section 1
Secure data with Zero Trust, section 1
SP 800-207, Zero Trust Architecture, page 9, section 3.2.1

QUESTION 3
Which security tools or capabilities can be utilized to automate the response to security events and incidents?

A. Single packet authorization (SPA)
B. Security orchestration, automation, and response (SOAR)
C. Multi-factor authentication (MFA)
D. Security information and event management (SIEM)

Correct Answer: B

Section:
Explanation:
SOAR is a collection of software programs developed to bolster an organization's cybersecurity posture. SOAR tools can automate the response to security events and incidents by executing predefined workflows or playbooks, which can include tasks such as alert triage, threat detection, containment, mitigation, and remediation. SOAR tools can also orchestrate the integration of various security tools and data sources, and provide centralized dashboards and reporting for security operations.
Reference=
Certificate of Competence in Zero Trust (CCZT) prepkit, page 23, section 3.2.2
Security Orchestration, Automation and Response (SOAR) - Gartner
Security Automation: Tools, Process and Best Practices - Cynet, section ''What are the different types of security automation tools?''
Introduction to automation in Microsoft Sentinel

QUESTION 4
Network architects should consider_____ before selecting an SDP model.
Select the best answer.

A. leadership buy-in
B. gateways
C. their use case
D. cost

Correct Answer: C
Section:
Explanation:
Different SDP deployment models have different advantages and disadvantages depending on the organization's use case, such as the type of resources to be protected, the location of the clients and servers, the network topology, the scalability, the performance, and the security requirements. Network architects should consider their use case before selecting an SDP model that best suits their needs and goals.
Reference=
Certificate of Competence in Zero Trust (CCZT) prepkit, page 21, section 3.1.2
6 SDP Deployment Models to Achieve Zero Trust | CSA, section ''Deployment Models Explained''
Software-Defined Perimeter (SDP) and Zero Trust | CSA, page 7, section 3.1
Why SDP Matters in Zero Trust | SonicWall, section ''SDP Deployment Models''

QUESTION 5
Which component in a ZTA is responsible for deciding whether to grant access to a resource?

A. The policy enforcement point (PEP)
B. The policy administrator (PA)
C. The policy engine (PE)
D. The policy component

Correct Answer: C
Section:
Explanation:
The policy engine (PE) is the component in a ZTA that is responsible for deciding whether to grant access to a resource. The PE evaluates the policies and the contextual data collected from various sources, such as the user identity, the device posture, the network location, the resource attributes, and the environmental factors, and then generates an access decision. The PE communicates the access decision to the policy enforcement point (PEP), which enforces the decision on the resource.
Reference=
Certificate of Competence in Zero Trust (CCZT) prepkit, page 14, section 2.2.2
What Is Zero Trust Architecture (ZTA)? - F5, section ''Policy Engine''
What is Zero Trust Architecture (ZTA)? | NextLabs, section ''Core Components''

[SP 800-207, Zero Trust Architecture], page 11, section 3.3.1

QUESTION 6
What is the function of the rule-based security policies configured on the policy decision point (PDP)?

A. Define rules that specify how information can flow
B. Define rules that specify multi-factor authentication (MFA) requirements
C. Define rules that map roles to users
D. Define rules that control the entitlements to assets

Correct Answer: D
Section:
Explanation:
Rule-based security policies are a type of attribute-based access control (ABAC) policies that define rules that control the entitlements to assets, such as data, applications, or devices, based on the attributes of the subjects, objects, and environment. The policy decision point (PDP) is the component in a zero trust architecture (ZTA) that evaluates the rule-based security policies and generates an access decision for each request.
Reference=
Certificate of Competence in Zero Trust (CCZT) prepkit, page 14, section 2.2.2
A Zero Trust Policy Model | SpringerLink, section ''Rule-Based Policies''
Zero Trust architecture: a paradigm shift in cybersecurity - PwC, section ''Security policy and control framework''

QUESTION 7
To respond quickly to changes while implementing ZT Strategy, an organization requires a mindset and culture of

A. learning and growth.
B. continuous risk evaluation and policy adjustment.
C. continuous process improvement.
D. project governance.

Correct Answer: B
Section:
Explanation:
To respond quickly to changes while implementing ZT Strategy, an organization requires a mindset and culture of continuous risk evaluation and policy adjustment. This means that the organization should constantly monitor the threat landscape, assess the security posture, and update the policies and controls accordingly to maintain a high level of protection and resilience. The organization should also embrace feedback, learning, and improvement as part of the ZT journey.
Reference=
Certificate of Competence in Zero Trust (CCZT) prepkit, page 7, section 1.3
Cultivating a Zero Trust mindset - AWS Prescriptive Guidance, section ''Continuous learning and improvement''
Zero Trust architecture: a paradigm shift in cybersecurity - PwC, section ''Continuous monitoring and improvement''

QUESTION 8
What is one of the key purposes of leveraging visibility & analytics capabilities in a ZTA?

A. Automatically granting access to all requested applications and data.
B. Ensuring device compatibility with legacy applications.
C. Enhancing network performance for faster data access.
D. Continually evaluating user behavior against a baseline to identify unusual actions.

Correct Answer: D

Section:
Explanation:
One of the key purposes of leveraging visibility & analytics capabilities in a ZTA is to continually evaluate user behavior against a baseline to identify unusual actions. This helps to detect and respond to potential threats, anomalies, and deviations from the normal patterns of user activity. Visibility & analytics capabilities also enable the collection and analysis of telemetry data across all the core pillars of ZTA, such as user, device, network, application, and data, and provide insights for policy enforcement and improvement.
Reference=
Certificate of Competence in Zero Trust (CCZT) prepkit, page 15, section 2.2.3
Zero Trust for Government Networks: 4 Steps You Need to Know, section ''Continuously verify trust with visibility & analytics''
The role of visibility and analytics in zero trust architectures, section ''The basic NIST tenets of this approach include''
What is Zero Trust Architecture (ZTA)? | NextLabs, section ''With real-time access control, users are reliably verified and authenticated before each session''

QUESTION 9
The following list describes the SDP onboarding process/procedure.
What is the third step? 1. SDP controllers are brought online first. 2.
Accepting hosts are enlisted as SDP gateways that connect to and authenticate with the SDP controller. 3.

A. Initiating hosts are then onboarded and authenticated by the SDP gateway
B. Clients on the initiating hosts are then onboarded and authenticated by the SDP controller
C. SDP gateway is brought online
D. Finally, SDP controllers are then brought online

Correct Answer: A
Section:
Explanation:
The third step in the SDP onboarding process is to onboard and authenticate the initiating hosts, which are the clients that request access to the protected resources. The initiating hosts connect to and authenticate with the SDP gateway, which acts as an accepting host and a proxy for the protected resources. The SDP gateway verifies the identity and posture of the initiating hosts and grants them access to the resources based on the policies defined by the SDP controller.
Reference=
Certificate of Competence in Zero Trust (CCZT) prepkit, page 21, section 3.1.2
6 SDP Deployment Models to Achieve Zero Trust | CSA, section ''Deployment Models Explained''
Software-Defined Perimeter (SDP) and Zero Trust | CSA, page 7, section 3.1

QUESTION 10
Which of the following is a common activity in the scope, prioritya nd business case steps of ZT planning?

A. Determine the organization's current state
B. Prioritize protect surfaces O C. Develop a target architecture
C. Identify business and service owners

Correct Answer: A
Section:
Explanation:
A common activity in the scope, priority, and business case steps of ZT planning is to determine the organization's current state. This involves assessing the existing security posture, architecture, policies, processes, and capabilities of the organization, as well as identifying the key stakeholders, business drivers, and goals for the ZT initiative. Determining the current state helps to establish a baseline, identify gaps and risks, and define the scope and priority of the ZT transformation.
Reference=
Zero Trust Planning - Cloud Security Alliance, section ''Scope, Priority, & Business Case''
The Zero Trust Journey: 4 Phases of Implementation - SEI Blog, section ''First Phase: Prepare''

QUESTION 11
Within the context of risk management, what are the essential components of an organization's ongoing risk analysis?

A. Gap analysis, security policies, and migration
B. Assessment frequency, metrics, and data
C. Log scoping, log sources, and anomalies
D. Incident management, change management, and compliance

Correct Answer: B
Section:
Explanation:
The essential components of an organization's ongoing risk analysis are assessment frequency, metrics, and data. Assessment frequency refers to how often the organization conducts risk assessments to monitor and measure the effectiveness of the zero trust architecture and policies. Metrics refer to the quantitative and qualitative indicators that are used to evaluate the security posture, performance, and compliance of the zero trust architecture. Data refers to the information that is collected, analyzed, and reported from various sources, such as telemetry, logs, audits, and feedback, to support risk analysis and decision making.
Reference=
Zero Trust Planning - Cloud Security Alliance, section ''Monitor & Measure''
How to improve risk management using Zero Trust architecture | Microsoft Security Blog, section ''Monitoring and reporting''
Zero Trust Adoption: Managing Risk with Cybersecurity Engineering and Adaptive Risk Assessment - SEI Blog, section ''Continuous Monitoring and Improvement''

QUESTION 12
ZTA reduces management overhead by applying a consistent access model throughout the environment for all assets. What can be said about ZTA models in terms of access decisions?

A. The traffic of the access workflow must contain all the parameters for the policy decision points.
B. The traffic of the access workflow must contain all the parameters for the policy enforcement points.
C. Each access request is handled just-in-time by the policy decision points.
D. Access revocation data will be passed from the policy decision points to the policy enforcement points.

Correct Answer: C
Section:
Explanation:
ZTA models in terms of access decisions are based on the principle of ''never trust, always verify'', which means that each access request is handled just-in-time by the policy decision points. The policy decision points are the components in a ZTA that evaluate the policies and the contextual data collected from various sources, such as the user identity, the device posture, the network location, the resource attributes, and the environmental factors, and then generate an access decision. The access decision is communicated to the policy enforcement points, which enforce the decision on the resource. This way, ZTA models apply a consistent access model throughout the environment for all assets, regardless of their location, type, or ownership.
Reference=
Certificate of Competence in Zero Trust (CCZT) prepkit, page 14, section 2.2.2
What Is Zero Trust Architecture (ZTA)? - F5, section ''Policy Engine''
Zero trust security model - Wikipedia, section ''What Is Zero Trust Architecture?''
Zero Trust Maturity Model | CISA, section ''Zero trust security model''

QUESTION 13
To successfully implement ZT security, two crucial processes must be planned and aligned with existing access procedures that the ZT implementation might impact. What are these two processes?

A. Incident and response management
B. Training and awareness programs
C. Vulnerability disclosure and patching management
D. Business continuity planning (BCP) and disaster recovery (DR)

Correct Answer: B
Section:

QUESTION 14
In a ZTA, the logical combination of both the policy engine (PE) and policy administrator (PA) is called

A. policy decision point (PDP)
B. role-based access
C. policy enforcement point (PEP)
D. data access policy

Correct Answer: A
Section:
Explanation:
In a ZTA, the logical combination of both the policy engine (PE) and policy administrator (PA) is called the policy decision point (PDP). The PE is the component that evaluates the policies and the contextual data collected from various sources and generates an access decision. The PA is the component that establishes or terminates the communication between a subject and a resource based on the access decision. The PDP communicates with the policy enforcement point (PEP), which enforces the access decision on the resource.
Reference=
Certificate of Competence in Zero Trust (CCZT) prepkit, page 14, section 2.2.2
Zero Trust Architecture Project - NIST Computer Security Resource Center, slide 9
What Is a Zero Trust Security Framework? | Votiro, section ''The Policy Engine and Policy Administrator''
Zero Trust Frameworks Architecture Guide - Cisco, page 4, section ''Policy Decision Point''

QUESTION 15
To ensure a successful ZT effort, it is important to

A. engage finance regularly so they understand the effort and do not cancel the project
B. keep the effort focused within IT to avoid any distractions
C. engage stakeholders across the organization and at all levels, including functional areas
D. minimize communication with the business units to avoid 'scope creep'

Correct Answer: C
Section:
Explanation:
To ensure a successful ZT effort, it is important to engage stakeholders across the organization and at all levels, including functional areas. This helps to align the ZT vision and goals with the business priorities and needs, gain buy-in and support from the leadership and the users, and foster a culture of collaboration and trust. Engaging stakeholders also enables the identification and mapping of the critical assets, workflows, and dependencies, as well as the communication and feedback mechanisms for the ZT transformation.
Reference=
Certificate of Competence in Zero Trust (CCZT) prepkit, page 7, section 1.3
Zero Trust Planning - Cloud Security Alliance, section ''Scope, Priority, & Business Case''
The 'Zero Trust' Model in Cybersecurity: Towards understanding and ..., section ''3.1 Ensuring buy-in across the organization with tangible impact''

QUESTION 16
Of the following, which option is a prerequisite action to understand the organization's protect surface clearly?

A. Data and asset classification
B. Threat intelligence capability and monitoring
C. Gap analysis of the organization's threat landscape

D. To have the latest risk register for controls implementation

Correct Answer: A
Section:
Explanation:
Data and asset classification is a prerequisite action to understand the organization's protect surface clearly because it helps to identify the most critical and sensitive data and assets that need to be protected by Zero Trust principles. Data and asset classification also helps to define the appropriate policies and controls for different levels of data and asset sensitivity.
Reference=Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance,Zero Trust Training (ZTT) - Module 2: Data and Asset Classification

QUESTION 17
For ZTA, what should be used to validate the identity of an entity?

A. Password management system
B. Multifactor authentication
C. Single sign-on
D. Bio-metric authentication

Correct Answer: B
Section:
Explanation:
Multifactor authentication is a method of validating the identity of an entity by requiring two or more factors, such as something the entity knows (e.g., password, PIN), something the entity has (e.g., token, smart card), or something the entity is (e.g., biometric, behavioral). Multifactor authentication enhances the security of Zero Trust Architecture (ZTA) by reducing the risk of identity compromise and unauthorized access.
Reference=Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance,Zero Trust Training (ZTT) - Module 4: Identity and Access Management

QUESTION 18
Scenario: An organization is conducting a gap analysis as a part of its ZT planning. During which of the following steps will risk appetite be defined?

A. Create a roadmap
B. Determine the target state
C. Determine the current state
D. Define requirements

Correct Answer: D
Section:
Explanation:
During the define requirements step of ZT planning, the organization will define its risk appetite, which is the amount and type of risk that it is willing to accept in pursuit of its objectives. Risk appetite reflects the organization's risk culture, tolerance, and strategy, and guides the development of the ZT policies and controls. Risk appetite should be aligned with the business priorities and needs, and communicated clearly to the stakeholders.
Reference=
Certificate of Competence in Zero Trust (CCZT) prepkit, page 7, section 1.3
Risk Appetite Guidance Note - GOV.UK, section ''Introduction''
How to improve risk management using Zero Trust architecture | Microsoft Security Blog, section ''Risk management is an ongoing activity''

QUESTION 19
Which activity of the ZT implementation preparation phase ensures the resiliency of the organization's operations in the event of disruption?

A. Change management process
B. Business continuity and disaster recovery

C. Visibility and analytics
D. Compliance

Correct Answer: B
Section:
Explanation:
Business continuity and disaster recovery are the activities of the ZT implementation preparation phase that ensure the resiliency of the organization's operations in the event of disruption. Business continuity refers to the process of maintaining or restoring the essential functions of the organization during and after a crisis, such as a natural disaster, a cyberattack, or a pandemic. Disaster recovery refers to the process of recovering the IT systems, data, and infrastructure that support the business continuity. ZT implementation requires planning and testing the business continuity and disaster recovery strategies and procedures, as well as aligning them with the ZT policies and controls.
Reference=
Zero Trust Planning - Cloud Security Alliance, section ''Monitor & Measure''
Zero Trust architecture: a paradigm shift in cybersecurity - PwC, section ''Continuous monitoring and improvement''
Zero Trust Implementation, section ''Outline Zero Trust Architecture (ZTA) implementation steps''

QUESTION 20
Which element of ZT focuses on the governance rules that define the 'who, what, when, how, and why' aspects of accessing target resources?

A. Policy
B. Data sources
C. Scrutinize explicitly
D. Never trust, always verify

Correct Answer: A
Section:
Explanation:
Policy is the element of ZT that focuses on the governance rules that define the ''who, what, when, how, and why'' aspects of accessing target resources. Policy is the core component of a ZTA that determines the access decisions and controls for each request based on various attributes and factors, such as user identity, device posture, network location, resource sensitivity, and environmental context. Policy is also the element that enables the ZT principles of ''never trust, always verify'' and ''scrutinize explicitly'' by enforcing granular, dynamic, and data-driven rules for each access request.
Reference=
Certificate of Competence in Zero Trust (CCZT) prepkit, page 14, section 2.2.2
What Is Zero Trust Architecture (ZTA)? - F5, section ''Policy Engine''
Zero Trust Architecture Project - NIST Computer Security Resource Center, slide 9
[Zero Trust Frameworks Architecture Guide - Cisco], page 4, section ''Policy Decision Point''

QUESTION 21
What does device validation help establish in a ZT deployment?

A. Connection based on user
B. High-speed network connectivity
C. Trusted connection based on certificate-based keys
D. Unrestricted public access

Correct Answer: C
Section:
Explanation:
Device validation helps establish a trusted connection based on certificate-based keys in a ZT deployment. Device validation is the process of verifying the identity and posture of the devices that request access to the protected resources. Device validation relies on the use of certificates, which are digital credentials that bind the device identity to a public key. Certificates are issued by a trusted authority and can be used to authenticate

the device and encrypt the communication. Device validation helps to ensure that only healthy and compliant devices can access the resources, and that the connection is secure and confidential.
Reference=
Certificate of Competence in Zero Trust (CCZT) prepkit, page 15, section 2.2.3
Zero Trust and Windows device health - Windows Security, section ''Device health attestation on Windows''
Devices and zero trust | Google Cloud Blog, section ''In a zero trust environment, every device has to earn trust in order to be granted access.''

QUESTION 22
Which approach to ZTA strongly emphasizes proper governance of access privileges and entitlements for specific assets?

A. ZTA using device application sandboxing
B. ZTA using enhanced identity governance
C. ZTA using micro-segmentation
D. ZTA using network infrastructure and SDPs

Correct Answer: B
Section:
Explanation:
ZTA using enhanced identity governance is an approach to ZTA that strongly emphasizes proper governance of access privileges and entitlements for specific assets. This approach focuses on managing the identity lifecycle, enforcing granular and dynamic policies, and auditing and monitoring access activities. ZTA using enhanced identity governance helps to ensure that only authorized and verified entities can access the protected assets based on the principle of least privilege and the context of the request.
Reference=Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance,Zero Trust Training (ZTT) - Module 5: Enhanced Identity Governance

QUESTION 23
During the monitoring and analytics phase of ZT transaction flowso rganizations should collect statistics and profile the behavior of transactions. What does this support in the ZTA?

A. Creating firewall policies to protect data in motion
B. A continuous assessment of all transactions
C. Feeding transaction logs into a log monitoring engine
D. The monitoring of relevant data in critical areas

Correct Answer: B
Section:
Explanation:
During the monitoring and analytics phase of ZT transaction flows, organizations should collect statistics and profile the behavior of transactions to support a continuous assessment of all transactions. A continuous assessment of all transactions means that the organization constantly evaluates the security posture, performance, and compliance of each transaction, and detects and responds to any anomalies, deviations, or threats. A continuous assessment of all transactions helps to maintain a high level of protection and resilience in the ZTA, and enables the organization to adjust and improve the policies and controls accordingly.
Reference=
Zero Trust Planning - Cloud Security Alliance, section ''Monitor & Measure''
The role of visibility and analytics in zero trust architectures, section ''The basic NIST tenets of this approach include''
Move to the Zero Trust Security Model - Trailhead, section ''Monitor and Maintain Your Environment''

QUESTION 24
When planning for a ZTA, a critical product of the gap analysis process is_____
Select the best answer.

A. a responsible, accountable, consulted, and informed (RACI) chart and communication plan
B. supporting data for the project business case
C. the implementation's requirements

D. a report on impacted identity and access management (IAM) infrastructure

Correct Answer: C
Section:
Explanation:
A critical product of the gap analysis process is the implementation's requirements, which are the specifications and criteria that define the desired outcomes, capabilities, and functionalities of the ZTA. The implementation's requirements are derived from the gap analysis, which identifies the current state, the target state, and the gaps between them. The implementation's requirements help to guide the design, development, testing, and deployment of the ZTA, as well as the evaluation of its effectiveness and alignment with the business objectives and needs.
Reference=
Zero Trust Planning - Cloud Security Alliance, section ''Scope, Priority, & Business Case''
The Zero Trust Journey: 4 Phases of Implementation - SEI Blog, section ''Second Phase: Assess''
Planning for a Zero Trust Architecture: A Planning Guide for Federal ..., section ''Gap Analysis''

QUESTION 25
ZT project implementation requires prioritization as part of the overall ZT project planning activities. One area to consider is_____
Select the best answer.

A. prioritization based on risks
B. prioritization based on budget
C. prioritization based on management support
D. prioritization based on milestones

Correct Answer: A
Section:
Explanation:
ZT project implementation requires prioritization as part of the overall ZT project planning activities. One area to consider is prioritization based on risks, which means that the organization should identify and assess the potential threats, vulnerabilities, and impacts that could affect its assets, operations, and reputation, and prioritize the ZT initiatives that address the most critical and urgent risks. Prioritization based on risks helps to align the ZT project with the business objectives and needs, and optimize the use of resources and time.
Reference=
Zero Trust Planning - Cloud Security Alliance, section ''Scope, Priority, & Business Case''
The Zero Trust Journey: 4 Phases of Implementation - SEI Blog, section ''Second Phase: Assess''
Planning for a Zero Trust Architecture: A Planning Guide for Federal ..., section ''Gap Analysis''

QUESTION 26
According to NIST, what are the key mechanisms for definingm anaging, and enforcing policies in a ZTA?

A. Policy decision point (PDP), policy enforcement point (PEP), and policy information point (PIP)
B. Data access policy, public key infrastructure (PKI), and identity and access management (IAM)
C. Control plane, data plane, and application plane
D. Policy engine (PE), policy administrator (PA), and policy broker (PB)

Correct Answer: A
Section:
Explanation:
According to NIST, the key mechanisms for defining, managing, and enforcing policies in a ZTA are the policy decision point (PDP), the policy enforcement point (PEP), and the policy information point (PIP). The PDP is the component that evaluates the policies and the contextual data collected from various sources and generates an access decision. The PEP is the component that enforces the access decision on the resource. The PIP is the component that provides the contextual data to the PDP, such as the user identity, the device posture, the network location, the resource attributes, and the environmental factors.
Reference=
Zero Trust Architecture Project - NIST Computer Security Resource Center, slide 9

What Is Zero Trust Architecture (ZTA)? - F5, section ''Policy Engine''
Zero Trust Frameworks Architecture Guide - Cisco, page 4, section ''Policy Decision Point''

QUESTION 27
When planning for ZT implementation, who will determine valid users, roles, and privileges for accessing data as part of data governance?

A. IT teams
B. Application owners
C. Asset owners
D. Compliance officers

Correct Answer: C
Section:
Explanation:
Asset owners are the ones who will determine valid users, roles, and privileges for accessing data as part of data governance. Asset owners are responsible for defining the data classification, sensitivity, and ownership of the data assets they own. They also have the authority to grant or revoke access to the data assets based on the business needs and the Zero Trust policies.
Reference=Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance,Zero Trust Training (ZTT) - Module 2: Data and Asset Classification

QUESTION 28
Which of the following is a potential outcome of an effective ZT
implementation?

A. Regular vulnerability scanning
B. A comprehensive catalogue of all transactions, dependencies, and services with associated IDs
C. Deployment of traditional firewall solutions
D. Adoption of biometric authentication

Correct Answer: B
Section:
Explanation:
A comprehensive catalogue of all transactions, dependencies, and services with associated IDs is a potential outcome of an effective ZT implementation because it helps to map the data flows and interactions among the assets and entities in the ZTA. This catalogue enables the ZTA to enforce granular and dynamic policies based on the context and attributes of the transactions, dependencies, and services. It also facilitates the monitoring and auditing of the ZTA activities and performance.
Reference=Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance,Zero Trust Training (ZTT) - Module 3: ZTA Architecture and Components

QUESTION 29
How can we use ZT to ensure that only legitimate users can access a SaaS or PaaS? Select the best answer.

A. Implementing micro-segmentation and mutual Transport Layer Security (mTLS)
B. Configuring the security assertion markup language (SAML) service provider only to accept requests from the designated ZT gateway
C. Integrating behavior analysis and geofencing as part of ZT controls
D. Enforcing multi-factor authentication (MFA) and single-sign on (SSO)

Correct Answer: B
Section:
Explanation:
(Configuring the security assertion markup language (SAML) service provider only to accept requests from the designated ZT gateway) Explanation: Configuring SAML to accept requests only from the designated ZT gateway ensures that all access requests are authenticated and authorized appropriately. Reference = Zero Trust Architecture related sources including NIST

QUESTION 30
What should be a key component of any ZT project, especially during implementation and adjustments?

A. Extensive task monitoring
B. Frequent technology changes
C. Proper risk management
D. Frequent policy audits

Correct Answer: C
Section:
Explanation:
Proper risk management should be a key component of any ZT project, especially during implementation and adjustments, because it helps to identify, analyze, evaluate, and treat the potential risks that may affect the ZT and ZTA objectives and outcomes. Proper risk management also helps to prioritize the ZT and ZTA activities and resources based on the risk level and impact, and to monitor and review the risk mitigation strategies and actions.
Reference=Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance,Zero Trust Training (ZTT) - Module 9: Risk Management

QUESTION 31
SDP incorporates single-packet authorization (SPA). After successful authentication and authorization, what does the client usually do next? Select the best answer.

A. Generates an SPA packet and sends it to the initiating host.
B. Generates an SPA packet and sends it to the controller.
C. Generates an SPA packet and sends it to the accepting host.
D. Generates an SPA packet and sends it to the gateway.

Correct Answer: B
Section:
Explanation:
After successful authentication and authorization, the client typically sends an SPA packet to the controller, which acts as an intermediary in authenticating the client's request before access to the accepting host is granted.
Reference = Certificate of Competence in Zero Trust (CCZT) - Cloud Security Alliance, Zero Trust Training (ZTT) - Module 9: Risk Management