CCZT Sample Questions

Check your knowledge before taking the exam

Introduction to Zero Trust Architecture

Q1: Which of the following are technical objectives of Zero Trust Architecture?

- Enable network scanning, centralize access management, expand attack surface
- Implement VPNs, maximize user privileges, remove network segmentation
- **Establish a protective framework, simplify user experience, reduce attack surface and complexity**
- Increase network visibility, share incident data publicly, allow implicit trust

***Justification**: The technical objectives of ZTA include establishing a protective framework, simplifying user experience, reducing attack surface and complexity, enforcing least privilege, improving security posture and resilience, and improving incident containment. The correct answer captures several of the key technical objectives.*

Q2: Which of the following are key business objectives of adopting a Zero Trust Architecture (ZTA)?

- **Reducing cyber risk, improving compliance management, and aligning organizational culture with ZT principles**
- Simplifying the enterprise IT architecture, reducing costs, and increasing user productivity
- Enabling secure remote access, replacing VPNs, and improving visibility into cloud environments
- Accelerating digital transformation, adopting cloud services, and enabling edge computing

***Justification**: The key business objectives of ZTA include reducing overall cyber risk, improving the organization's compliance posture, and fostering a culture of continuous verification aligned with ZT principles.*

Q3: What are some key risks to consider when implementing Zero Trust Architecture (ZTA) in a project?

- Reduced management overhead compared to legacy architectures
- Improved incident containment capabilities

- Incompatibility with cloud-based infrastructure and services
- **Failure of operational ZTA elements like policy decision points or policy enforcement points**

Justification: Failure of critical ZTA components can hinder proper authentication and access to secured assets, compromising security.

Q4: According to NIST SP 800-207, which of the following are the three main approaches for implementing a Zero Trust Architecture?

- **Enhanced identity governance, micro-segmentation, and software-defined perimeters (SDP)**
- Network segmentation, multi-factor authentication, and cloud access security brokers
- Identity and access management, continuous monitoring, and data encryption
- Least privilege access, network access control, and endpoint detection and response

***Justification**: NIST SP 800-207 outlines three main approaches for implementing ZTA: using enhanced identity governance, using micro-segmentation, and using network infrastructure and SDPs. These approaches cover identity, network, and perimeter aspects of ZTA.*

Q5: What is CSA's SDP approach designed to enable through on-demand, dynamically provisioned isolated networks?

- Elimination of the need for network segmentation
- **Enforcement of Zero Trust principles**
- Replacement of firewalls with software-based controls
- Increased network visibility for all connected devices

***Justification**: CSA's SDP is an approach to enable and enforce Zero Trust principles by providing on-demand, dynamically provisioned networks isolated from unsecured networks to mitigate network-based attacks.*

Q6: What are some limitations of zero trust architecture when it comes to legacy systems, unmanaged devices, and integration?

- ZTA is incompatible with legacy systems and cannot be used with unmanaged devices under any circumstances.
- ZTA integration will always introduce significant latency and performance degradation, especially for legacy systems.
- **ZTA may be difficult to fully implement for legacy systems and unmanaged devices, requiring careful integration to minimize latency**
- Legacy systems and unmanaged devices are easily integrated into ZTA implementations with no special considerations needed.

***Justification**: Legacy systems and unmanaged devices can pose challenges for fully realizing ZTA and may require additional effort to integrate while avoiding performance impacts. Careful planning is needed.*

Q7: What was a key emphasis of Zero Trust when it was first coined by John Kindervag around 2010?

- Network traffic inside the perimeter can be trusted by default
- Requests only need a single verification at the network perimeter
- Trusted users should be granted broad access without re-verification
- **All network traffic is untrusted and requests need verification at each step**

***Justification**: Kindervag emphasized that all network traffic is untrusted. His position was that all requests to access data or resources should be verified at each step.*

Q8: Which of the following best describes the Zero Trust concept as defined by CSA?

- **Making no assumptions about trustworthiness, starting with no entitlements, and verifying all access**
- Trusting internal network traffic by default while verifying external access
- Granting entitlements upfront based on user roles and verifying as needed
- Verifying access only for resources deemed high-risk or business critical

***Justification**: CSA defines Zero Trust as requiring no assumptions about trustworthiness, starting with no pre-established entitlements, and verifying all access to resources regardless of location.*

Q9: Which of the following are included in the ZTA design principles?

- Implicitly trusting devices inside the network perimeter
- Allowing full access privileges to authorized users by default
- **Denying access until the requestor has been authenticated and authorized**
- Relying on one-time validation of security controls

***Justification**: ZTA design principles include denying access until authentication and authorization, allowing access only after authorization, enforcing least privilege, and requiring continuous monitoring.*

Q10: The key logical components of a ZTA include which of the following?

- Firewalls, intrusion detection systems, and VPNs
- **Policy decision point, policy enforcement point, and data sources**
- Identity providers, cloud access security brokers, and micro-segmentation
- Initiating hosts, accepting hosts, and SDP gateways

***Justification**: The PDP, PEP, and data sources that maintain updated access rules are the key logical components that make up a zero trust architecture according to NIST SP 800-207.*

Introduction to Software Defined Perimeter

Q11: What are the key issues that SDP addresses in traditional network security architectures?

- Preventing all cyber attacks, replacing firewalls, and eliminating the need for IAM
- Enabling secure internet access, replacing VPNs, and securing physical network ports
- **The changing perimeter, IP address challenges, and integrating security controls**
- Preventing misconfiguration, applying security patches, and monitoring network traffic

***Justification**: SDP was designed to solve challenges with the shifting network perimeter in cloud and mobile environments, the inadequacies of using IP addresses for security, and the difficulty of integrating disparate security controls in traditional architectures.*

Q12: How can SDP replace or complement existing industry solutions to overcome their limitations?

- **SDP integrates controls for firewalls, encryption, IAM, session management, and device management**
- SDP completely replaces firewalls, eliminating the need for any perimeter security
- SDP focuses solely on encryption and has no impact on identity and access management systems
- SDP eliminates the need for any device management by treating all devices as untrusted

***Justification**: SDP brings together multiple controls that are usually separated by function, integrating them into a comprehensive security architecture to establish and ensure secure connections.*

Q13: Which of the following are the three core tenets of Software-Defined Perimeter (SDP)?

- Trust but verify, limit access, and monitor continuously
- Integrate controls, automate security, and enable visibility
- Authenticate first, secure the perimeter, and restrict protocols
- **Assume nothing, trust no one or thing, and validate everything**

***Justification**: SDP is built on the core principles of zero trust - assuming nothing can be trusted, not trusting any entity by default, and always verifying and validating everything before granting access.*

Q14: Which of the following are underlying technologies that SDP relies on to provide its security capabilities?

- Intrusion detection systems, VPNs, multi-factor authentication, and DNS security extensions
- **Drop-all firewalls, separate control/data planes, mutual TLS, and single packet authorization**
- Role-based access control, OAuth authentication, containerization, and endpoint detection and response
- Network access control lists, SSL encryption, host-based firewalls, and security information and event management

***Justification**: SDP uses these core technologies together to provide its network security architecture. Drop-all firewalls block all traffic by default. Separate control and data planes allow authentication before network access. Mutual TLS encrypts communications. Single packet authorization pre-authorizes connections.*

Q15: Which of the following are key components of the SDP architecture?

- **Initiating hosts, accepting hosts, gateways, SDP clients, and the controller**
- Firewalls, intrusion detection systems, and VPNs
- SAML identity providers, LDAP directories, and Kerberos key distribution centers
- Cloud access security brokers, endpoint detection and response, and SIEMs

***Justification**: The key components of the SDP architecture include initiating hosts that initiate connections, accepting hosts that accept connections and provide protected services, gateways that provide access through the invisible perimeter, SDP clients installed on initiating host devices, and the controller that authenticates and authorizes connections.*

Q16: What does the SDP secure workflow involve to establish communications between the initiating host and accepting host?

- Controller activating hosts first, cloaking the IH, single mTLS handshake, no SPA exchange
- IH and AH connecting directly without a controller, no cloaking, SPA exchange after mTLS handshakes
- **Cloaking the AH, controller connecting to IAM, SPA exchange, separate mTLS handshakes for control and data planes**
- Cloaking the IH and AH, no IAM integration, combined mTLS handshake for control and data, no SPA

***Justification**: The SDP secure workflow involves the accepting host being cloaked, the controller connecting to IAM services, hosts being activated, SPA packets being exchanged to establish communications, and separate mTLS handshakes for the control and data planes.*

Q17: What are some key architectural considerations when deploying SDP?

- Replacing all existing firewalls, simplifying user access, minimizing logging, and allowing any device to connect
- **IAM (Identity and Access Management)**
- Eliminating DevOps practices, avoiding cloud environments, and prohibiting remote access
- Relying solely on perimeter firewalls, enabling unrestricted user access, and minimizing integration with existing identity and access management systems

***Justification**: SDP deployments must account for how they integrate with an organization's existing networks, systems, processes, and user experiences. Monitoring, logging, onboarding and device validation are also critical considerations.*

Q18: What is the key benefit of SDP's drop-all firewall that helps reduce an organization's attack surface?

- It analyzes packets more thoroughly than traditional firewalls
- It can inspect encrypted traffic without decrypting it
- It is cheaper and easier to configure than other types of firewalls
- **It only allows approved actions, rather than trying to block all unapproved actions**

***Justification**: The drop-all firewall operates on a least privilege model, dropping all traffic not explicitly allowed. This greatly reduces the attack surface by focusing security on allowing approved actions only.*

Q19: What is the primary purpose of the SDP architecture in integrating multiple security controls?

- **To establish and ensure secure connections across applications, firewalls, clients, etc.**
- To replace all traditional security tools and eliminate the need for firewalls and IAM
- To provide a new type of firewall that can secure connections without any other controls
- To encrypt all data at rest across the entire IT infrastructure of an organization

***Justification**: SDP unifies security controls that are usually separated by function, like applications, firewalls, and clients, in order to establish and guarantee secure connections.*

Q20: What are some key challenges that SDP helps organizations address when securing their expanding IT environments?

- Securing mainframe systems, AS/400 servers, and token ring networks
- **Securing physical networks, private/public clouds, SDNs, mobile workforce, and IT/OT convergence**
- Securing smart toilets, intelligent blenders, and self-driving toasters
- Securing employee personal devices, public Wi-Fi hotspots, and personal cloud storage

Justification: *SDP provides a way to unify security controls and policies across diverse and expanding IT environments, including physical networks, cloud deployments, SDNs, mobile users, and converged IT/OT systems.*

Zero Trust Strategy

Q21: What should be the primary focus when identifying and prioritizing protect surfaces in a Zero Trust implementation?

- Defending against all potential threats and attack vectors
- Replacing the entire existing infrastructure with new Zero Trust tools
- Applying Zero Trust controls uniformly across the entire network
- **Securing critical data, applications, assets and services (DAAS)**

Justification: *Protect surfaces contain an organization's most critical and vulnerable DAAS components. Identifying and securing these should be the top priority in a Zero Trust implementation.*

Q22: Which of the following is an important objective of mapping transaction flows in a Zero Trust implementation?

- **To determine optimal placement of controls for data protection**
- To identify all potential attack vectors
- To eliminate the need for network segmentation
- To replace the need for access controls

Justification: *Mapping transaction flows for each protect surface is critical for understanding data movement and determining where controls should be placed to best protect the data.*

Q23: Which of the following is a key challenge in adopting Zero Trust for an organization with legacy systems and infrastructure?

- Legacy systems always require immediate Zero Trust upgrades
- Legacy infrastructure has no impact on adopting Zero Trust models
- **Limited network and asset visibility hinders the transition to Zero Trust**
- Organizations with less mature measurement programs adapt to Zero Trust more easily

Justification: *Organizations with legacy systems often face challenges in adopting Zero Trust due to limited visibility into their network and assets. This lack of visibility makes it difficult to implement the granular access controls and continuous monitoring required for Zero Trust.*

Q24: What is a key consideration when aligning a Zero Trust strategy with organizational drivers and values?

- **Understanding how Zero Trust adoption offers competitive advantages like streamlined security and cost reduction**
- Ensuring Zero Trust controls do not impact user productivity or add friction to business processes
- Selecting specific Zero Trust technologies and solutions to implement across the organization
- Assigning dedicated personnel to manage the Zero Trust implementation project

***Justification**: Demonstrating how Zero Trust aligns with and delivers on the organization's strategic objectives is crucial for gaining buy-in and support from key stakeholders.*

Q25: Why might legacy systems and infrastructure pose challenges for implementing Zero Trust?

- Legacy systems are incompatible with Zero Trust principles and cannot be included in a Zero Trust architecture
- Legacy systems have sufficient visibility and control, making Zero Trust implementation straightforward
- **Legacy systems may have technical constraints that require specialized strategies for Zero Trust implementation**
- All legacy systems must be immediately upgraded to enable Zero Trust, regardless of strategic considerations

***Justification:** Legacy systems like OT, IoT or ICS devices often have significant technical limitations in areas like patching and access control, necessitating specialized approaches to achieve Zero Trust objectives for such infrastructure.*

Q26: What is a key principle for maintaining the integrity and resilience of Zero Trust environments?

- Relying primarily on manual processes and human intervention
- **Automation, orchestration, and infrastructure as code play critical roles**
- Implementing a traditional network perimeter security model
- Granting implicit trust to devices within the corporate network

***Justification:** Automation, orchestration, and IaC enable continuous compliance checks against ZT policies, prevent config drift, and allow rapid response to threats by adjusting access controls in real-time.*

Q27: What is a key tenet of Zero Trust that assumes malicious actors reside both inside and outside of any network you manage?

- Never trust, always verify
- Presume breach

- Grant least privilege access
- **Assume a hostile environment**

Justification: *One of the key tenets of Zero Trust is to assume a hostile environment, recognizing that malicious actors can exist both inside and outside the network perimeter.*

Q28: Why is alignment with business functions and compliance requirements important for Zero Trust implementation?

- It allows the organization to ignore compliance requirements in favor of Zero Trust principles
- It ensures Zero Trust is implemented exactly the same way across all business functions
- **It ensures that Zero Trust practices adhere to regulations while supporting the organization's objectives**
- It mandates that compliance audits are no longer necessary after Zero Trust adoption

Justification: *Aligning Zero Trust with business functions and compliance requirements ensures regulatory adherence and that security enables rather than hinders business operations. It requires an architecture allowing flexibility for different administrative controls, audit requirements, and certifications.*

Q29: What is the primary goal when defining the desired state for Zero Trust adoption in an organization?

- Fully replacing existing cybersecurity infrastructure and processes
- **Securing buy-in from key stakeholders within the organization**
- Creating a standardized Zero Trust roadmap for all organizations
- Focusing solely on the technical components of Zero Trust Architecture

Justification: *The central objective when defining the desired Zero Trust state is to secure buy-in from key stakeholders. This ensures the Zero Trust strategy is not only well-conceived but also well-received and integrated within the organization.*

Q30: What are the five key steps for implementing a Zero Trust architecture according to the Cloud Security Alliance?

- **Define protect surfaces, map transaction flows, build ZTA, create ZT policy, monitor and maintain**
- Identify risks, design network segments, implement controls, train users, audit compliance
- Assess current state, set goals, deploy tools, enforce policies, measure effectiveness
- Inventory assets, classify data, update systems, restrict access, enable monitoring

Justification: *The Cloud Security Alliance outlines these five essential steps for operationalizing each protect surface project when implementing a Zero Trust architecture. They provide a structured approach to enhance cybersecurity and ensure a successful transition to a Zero Trust paradigm.*

Zero Trust Planning

Q31: Which role is most critical in a Zero Trust implementation for determining access privileges as part of their data governance responsibilities?

- Asset custodian
- End users
- IT administrators
- **Asset owner**

***Justification**: The asset owner resides in the business units and determines valid users, roles, privileges, and data usage as part of their data governance role, making them the most critical Zero Trust-specific role.*

Q32: What inventories potential risk events and controls to reduce risk within defined appetite thresholds?

- **A risk register**
- A configuration management database (CMDB)
- A business impact assessment (BIA)
- A data classification policy

***Justification**: A risk register inventories potential risk events and controls to reduce risk levels within the organization's defined risk appetite thresholds.*

Q33: Which of the following should be identified early in Zero Trust planning to determine potential impacts or updates needed?

- Workforce training needs
- Desired target CISA maturity stage
- **Architecture capabilities and components**
- Attack surface monitoring tools

***Justification**: Architecture capabilities and components that could impact Zero Trust or require updates should be identified early in the planning process to understand the scope and effort required.*

Q34: How can implementing a Zero Trust approach help organizations comply with existing cybersecurity and data privacy regulations?

- By eliminating the need for organizations to comply with any regulations
- By providing a checklist of all the specific Zero Trust regulatory requirements
- By automatically reporting an organization's Zero Trust status to regulators
- **By increasing control over regulated data and driving better overall cybersecurity**

Justification: *Zero Trust increases control over regulated data through enforcing accountability and data segregation. It also drives better overall cybersecurity which often exceeds existing legal and regulatory requirements.*

Q35: How should organizations prioritize their Zero Trust efforts?

- **Based on complexity, risks, or use cases, with a business case to justify the project**
- Randomly select protect surfaces to implement Zero Trust
- Tackle the most complex protect surfaces first to get them out of the way
- Prioritize based solely on available budget without considering other factors

Justification: *Prioritizing ZT efforts can be based on factors like starting simple and progressing to complex, addressing high-risk protect surfaces first, or focusing on specific use cases. The business case should outline costs, benefits, and risks to justify the project.*

Q36: What is a crucial prerequisite step before defining the scope of a Zero Trust implementation project?

- Identifying all the stakeholders who need to be involved in the Zero Trust planning process
- **Conducting data/asset discovery and classification to understand what needs to be protected**
- Performing a gap analysis to determine the organization's current Zero Trust maturity level
- Developing a business case to justify the investment in Zero Trust security controls

Justification: *Before defining the scope, data/asset discovery and classification is needed to understand what to protect with a ZT approach.*

Q37: Which of the following best describes who is responsible for planning and maintaining Zero Trust policies that regulate visibility and access based on various attributes?

- The identity provider
- **A policy administrator**
- The Policy Enforcement Point
- The data owner

Justification: *ZT policies regulate visibility and access based on various attributes. The policies are planned and maintained by a policy administrator, which is a logical component of the Policy Decision Point (PDP).*

Q38: What are two key benefits of defining the protect surface when planning a Zero Trust implementation**?**

- Defining the protect surface eliminates the need for network segmentation and logging
- It expands visibility of all entry points and is more comprehensive than the attack surface
- Defining the protect surface identifies the critical data and assets to protect
- **It allows moving controls closer to critical assets and is more stable than the attack surface**

***Justification**: Defining the protect surface allows security controls to be placed close to critical assets. The protect surface also remains more constant compared to the evolving, harder to define attack surface.*

Q39: Which of the following should form the basis of any Zero Trust approach to minimize project failure and disruption to existing systems?

- **Proper risk management**
- Extensive user training
- Rapid deployment timelines
- Reliance on existing controls

***Justification**: Establishing a risk management framework for identifying and mitigating risks is crucial for minimizing project failure and disruption to existing systems when implementing Zero Trust.*

Q40: Which of the following are key planning considerations for implementing a Zero Trust architecture?

- Open ports, privileged access for all users, on-premises infrastructure only
- Static security policies, annual risk assessments, perimeter-based network segmentation
- **Stakeholders, technology strategy, risk register, security policies, and architecture options**
- Default allow access policies, user training optional, focus on detection over prevention

***Justification**: Planning for Zero Trust requires engaging the right stakeholders, aligning with the overall technology strategy, understanding risks, updating security policies, and evaluating architecture options to best support Zero Trust principles.*

Zero Trust Implementation

Q41: Which of the following is a special consideration for implementing Zero Trust in BYOD environments?

- **Privacy concerns when deploying Zero Trust agents on personal devices**
- Ensuring devices support browser-based Zero Trust access methods
- Testing Zero Trust agents for compatibility with different operating systems
- Configuring Zero Trust policies based on device ownership

***Justification**: In BYOD environments, deploying Zero Trust agents on personal devices raises privacy concerns that need to be addressed, such as adding appropriate privacy notices in accordance with local laws.*

Q42: Which Zero Trust cross-cutting capability aggregates logs from ZT components to enable dashboards, event correlation, threat analysis and policy monitoring?

- Automation and Orchestration
- Governance
- Identity
- **Visibility and Analytics**

***Justification**: The Visibility and Analytics capability aggregates logs from various ZT components to provide dashboards, event correlation, threat analysis, and policy monitoring capabilities. This enables better visibility and analytics across the ZT architecture.*

Q43: What is the purpose of a formal governance review process in the context of Zero Trust implementations?

- To validate the technical details of the Zero Trust architecture design
- **To verify phase completion, funding, risk assessment and measurement of defined metrics**
- To ensure end users are trained on the new Zero Trust procedures
- To test the performance and scalability of the Zero Trust infrastructure components

***Justification**: The formal governance review process establishes checkpoints to ensure each implementation phase is completed successfully, sufficient funding exists for the next phase, risks are assessed, and defined metrics are measured to track progress.*

Q44: What should be done to existing transaction flows when implementing Zero Trust Architecture?

- Completely discard them and design new transaction flows from scratch
- Keep them as-is with no changes required for Zero Trust implementation
- **Review and remap them to incorporate Zero Trust nodes, services, and components**
- Document them for reference but don't modify the actual flow of transactions

***Justification**: Existing transaction flows must be reviewed and updated to include the necessary Zero Trust components like policy decision points and policy enforcement points. Transaction inventories should be maintained for each protect surface.*

Q45: Which of the following best describes how ZT implementations should drive future adjustments as the environment evolves?

- **Leverage a continuous feedback loop to monitor results and trigger change control**
- Once implemented, a ZT architecture should remain static to maintain security
- Adjust ZT implementations on an annual basis during scheduled maintenance windows
- Empower individual teams to make ad-hoc changes to ZT as they see fit

***Justification**: ZT implementations should utilize a continuous feedback loop to drive future adjustments. As the environment evolves, risk management should trigger change control to ensure the ZT implementation stays aligned with goals and requirements.*

Q46: When closing a Zero Trust implementation project, which of the following activities are critical to ensuring a successful transition to operations and maintenance?

- Decommissioning all legacy architecture, conducting vulnerability scans, and performing regular audits
- **Obtaining stakeholder sign-off, communicating the go-live date, and ensuring documentation is sufficient for future troubleshooting**
- Re-evaluating risks, making timeline adjustments, and reviewing technology changes
- Defining success criteria, promoting cross-departmental collaboration, and integrating with the cybersecurity program

***Justification**: Successful project closure requires key stakeholder sign-off, a communicated go-live date, and documentation to enable future maintenance and troubleshooting of the implemented Zero Trust solution.*

Q47: Which of the following are key implementation preparation activities for Zero Trust?

- Conducting penetration testing, reviewing SLAs with vendors, and rolling out ZT to the entire organization
- Identifying policy decision points, creating data flow diagrams, and decommissioning legacy systems
- **Defining project deliverables, communicating changes to users, and creating an implementation checklist**
- Performing a risk assessment, defining KPIs for success measurement, and implementing all ZT pillars simultaneously

Justification: *Key ZT implementation preparation activities include defining project deliverables to establish goals, communicating changes to users to prepare them, and creating a comprehensive implementation checklist covering governance, compliance, risk management, operations, analytics, incident management, change management, vulnerability management, BCP/DR, and training.*

Q48: How should a Zero Trust target architecture implementation leverage the five ZT pillars and three cross-cutting capabilities?

- Implement each pillar and capability sequentially and in isolation
- Focus only on the five pillars; the cross-cutting capabilities are optional
- Let each pillar team independently decide their own implementation approach
- **Define and prioritize implementation tasks across all pillars and capabilities**

Justification:*Ideally, all pillars and cross-cutting capabilities should be worked on simultaneously while following the five-step process outlined in the Zero Trust Strategy and Planning Study Guides.*

Q49: How should permissions for identities evolve as Zero Trust implementations mature from traditional to optimal levels?

- Permissions should remain role-based at all maturity levels
- **Permissions should transition from role-based to attribute-based as implementations mature**
- Permissions should be attribute-based at the start and transition to role-based
- Permissions do not need to change as Zero Trust implementations mature

Justification: *As Zero Trust implementations progress through the maturity levels from traditional to optimal, permissions for identities should evolve from role-based access to more granular, attribute-based access policies. This enables more precise control over access based on identity attributes.*

Q50: In a Zero Trust Architecture, which of the following tasks are required to effectively apply Zero Trust principles to data resources?

- Define transaction flows only for sensitive data resources
- Ship logs from the PDP and PEP to separate SIEMs for each resource
- **Discover, inventory, categorize, and control data resources**
- Use the identity store only to identify privileged users' data access

***Justification**: To apply Zero Trust to data, it is necessary to discover data resources, create an inventory, categorize or label the data, and implement controls to protect it. This allows making access decisions close to the data resource itself.*