IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **IdentityIQ-Associate**

Title : SailPoint Certified IdentityIQ Associate Exa

Version : DEMO

1.Is this statement true for the Edit Identity QuickLink?
It is used to view details about an identity.
A. Yes
B. No
Answer: B
Explanation:
The statement is false. The Edit Identity QuickLink is not intended merely to view identity details; its purpose is to initiate an identity modification request. In IdentityIQ, QuickLinks are request-entry mechanisms that expose controlled actions to users based on QuickLink Population rules, capabilities, request configuration, and target permissions. The Edit Identity QuickLink allows an authorized user to update configured identity attributes, typically through a form-driven request process that may include validation, approval, audit tracking, and workflow execution.
Viewing identity details is a separate functional concept. Identity information is normally reviewed through identity search, identity warehouse views, certification access review context, or identity detail pages, where the user can inspect IdentityCube data such as attributes, accounts, roles, entitlements, manager, and policy violations. Edit Identity may display current values so the requester understands what is being changed, but display is contextual, not the primary function.
Therefore, “It is used to view details about an identity” describes a view-oriented function, not the Edit Identity QuickLink.
Reference topics: User-Driven Requests, QuickLink Populations, create/edit/self-service identity requests, Identity Modeling, and IdentityCube usage.

2.Is this a purpose of identity governance and administration (IGA)?
Recording which data a user downloads
A. Yes
B. No
Answer: B
Explanation:
Recording which data a user downloads is not a core purpose of Identity Governance and Administration in SailPoint IdentityIQ. IGA is concerned with governing identities, accounts, access, entitlements, roles, policy violations, certifications, access requests, and provisioning. Its central objective is to answer questions such as who a user is, what access they have, whether that access is appropriate, who approved it, and whether access complies with defined business and security policies.
Tracking the specific files, records, or data objects downloaded by a user is typically associated with data activity monitoring, data loss prevention, security information and event management, or user behavior analytics. IdentityIQ may integrate with other systems and can govern access to applications or repositories that contain sensitive data, but it does not primarily function as a tool for recording every data download event.
In IdentityIQ terms, the governance focus is identity security: access visibility, access certification, policy enforcement, role modeling, lifecycle management, and provisioning controls.
Reference topics: Foundational Concepts, purpose of identity security, common IdentityIQ terms, governance model, certifications, policies, and provisioning.

3.Is this a purpose of identity governance and administration (IGA)?

Detecting and addressing inappropriate access
A. Yes
B. No
Answer: A
Explanation:
Detecting and addressing inappropriate access is a core purpose of Identity Governance and Administration in SailPoint IdentityIQ. IdentityIQ is designed to provide visibility into who has access, what access they have, how that access was obtained, whether it is appropriate, and what corrective action should occur when access violates business or security policy. Inappropriate access may be identified through access certifications, policy violations, role analysis, entitlement review, account aggregation, and identity correlation.
IdentityIQ supports this purpose by building IdentityCubes that consolidate identity, account, entitlement, role, and manager data from connected applications. Once access is visible, governance controls such as certifications allow managers, application owners, or entitlement owners to approve, revoke, or delegate access decisions. Policies can also detect toxic combinations, prohibited access, or access inconsistent with business rules. Remediation can then be routed through provisioning, work items, or manual fulfillment processes.
Therefore, the statement aligns directly with IGA and IdentityIQ's identity security model.
Reference topic: Foundational Concepts — purpose of identity security; also related to Governance — certifications, policy detection, and remediation.

4.Is this a purpose of identity governance and administration (IGA)?
Defining corporate reporting hierarchies
A. Yes
B. No
Answer: B
Explanation:
Defining corporate reporting hierarchies is not a primary purpose of Identity Governance and Administration. In SailPoint IdentityIQ, reporting hierarchy data is typically consumed from an authoritative source, such as an HR system, rather than created as the central objective of IGA. IdentityIQ may use manager relationships for identity correlation, access reviews, approval routing, escalation, lifecycle processing, and certification ownership, but the system's purpose is not to design or maintain the enterprise organizational chart.
IGA focuses on identity security outcomes: determining who users are, what access they have, whether that access is appropriate, how access was granted, and how inappropriate or risky access should be remediated. Manager and reporting-line data supports these controls, but it is supporting identity context, not the governance objective itself.
For example, a manager attribute may be used during Identity Refresh, certification generation, or access request approval. However, the business function of defining the reporting hierarchy normally remains with HR or organizational management systems.
Reference topics: Foundational Concepts — purpose of identity security; Identity Modeling — manager correlation and IdentityCube attributes; Governance — certification ownership and approval routing.

5.Is this a use of the data provided by the entitlement catalog?

Provide entitlement descriptions for viewing on the application definition.
A. Yes
B. No
Answer: B
Explanation:
The statement is not a correct use case for entitlement catalog data. In SailPoint IdentityIQ, the entitlement catalog is used to govern and enrich entitlement data after entitlements are discovered from application account/group schemas and aggregation. The catalog stores managed entitlement metadata such as display name, description, owner, classification, requestability, risk-related information, and other governance attributes. This information supports access reviews, access requests, approvals, role modeling, policy analysis, and decision-making by presenting business-readable information about technical access.
The application definition is primarily the configuration object for connecting to a target system. It contains connector settings, schemas, correlation configuration, aggregation options, provisioning settings, and related application-level controls. While entitlement-related configuration begins with the application schema, the entitlement catalog is not principally used to provide descriptions “for viewing on the application definition.” Its governed data is used in operational governance contexts, especially where reviewers, requesters, approvers, and administrators need understandable access context.
Therefore, entitlement descriptions are catalog governance metadata, not a feature whose purpose is simply display on the application definition.
Reference topics: Access Modeling — purpose of the entitlement catalog; Applications — group/account schemas; Governance — certification decision support; User-Driven Requests — access request display and approval context.