# Saviynt IGA Certified Professional Exam (L100)

## Saviynt SAVIGA-C01

**Version Demo**

**Total Demo Questions: 7**

**Total Premium Questions: 76**

**Buy Premium PDF**

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

The Sales department of a company requires an approval workflow to be created for an application where the Manager's approval should be followed by the Application Owner's approval. Which of the following sequences form the correct order of the workflow events?

**A.** Start > Resource Owner's Approval > Manager's Approval > Approve/Reject > End

**B.** Start > Manager's Approval > Custom Assignment > Approve/Reject > End

**C.** Start > Manager's Approval > Access Approval > Approve/Reject > End

**D.** Start > Manager's Approval > Resource Owner's Approval > Approve/Reject > End

**ANSWER: D**

**Explanation:**

"Start > Manager's Approval > Resource Owner's Approval > Approve/Reject > End" is the correct workflow sequence because it implements the stated serial approval requirement in the required order. The workflow begins with the request entering the approval process, then routes it to the requesting user's manager. Once the manager has approved, the request proceeds to the resource owner approval event. For an application-related request, the resource owner represents the accountable owner for the target resource or application and is therefore the appropriate workflow participant for the Application Owner approval requirement. After both required approvals have completed, the workflow reaches the Approve/Reject decision event, which determines the final outcome of the request and allows the process to end. This ordered design ensures that the application owner is not asked to act until the manager's approval has been provided, matching the business requirement precisely. Saviynt's workflow capability supports configuring approval routing and sequential approval stages for access-request processes; see the Saviynt Support Portal and Saviynt's Identity Governance and Administration product information.

**QUESTION NO: 2 - (SIMULATION)**

Match the following SoD Violations status with their description.

**ANSWER: Check the explanation for the answer**

**Explanation:**

The correct SoD Violation status matches are:

**Closed** — SoD violations that are closed, with or without remediation.
**Open** — SoD violations that require immediate attention.
**Risk Accepted** — SoD violations for which mitigation controls have been applied.
**In Process** — SoD violations that have been assigned.

In particular, **In Process** indicates an owner or assignee is working the violation, whereas **Risk Accepted** means the risk is formally accepted with compensating/mitigating controls.

**QUESTION NO: 3**

A Workday-RAAS user import mapping contains the following entry:

```
"SYSTEMUSERNAME": "wd:User_Name~#~string"
```

Which statement correctly describes this mapping?

**A.** SYSTEMUSERNAME is the Saviynt destination attribute, and wd:User_Name is the Workday source attribute.

**B.** SYSTEMUSERNAME is the Workday source attribute, and wd:User_Name is the Saviynt destination attribute.

**C.** SYSTEMUSERNAME is an endpoint attribute, and wd:User_Name is an entitlement attribute.

**D.** SYSTEMUSERNAME identifies the Workday report, and wd:User_Name identifies the response path.

**ANSWER: A**

**Explanation:**

**SYSTEMUSERNAME is the Saviynt destination attribute, and wd:User_Name is the source attribute in the Workday RaaS response.** In a Saviynt user import mapping, the attribute on the left side of the mapping is the Saviynt user attribute to be populated. The expression on the right side identifies the source value retrieved from the connected system.

The `wd:` prefix identifies the Workday XML namespace, so `wd:User_Name` is read from the Workday report output. The value is then stored in the Saviynt `SYSTEMUSERNAME` field. Reversing this direction would result in an incorrect interpretation of the mapping configuration.

## QUESTION NO: 4

Which of the following options support Authentication Mechanisms in Saviynt?

**A.** None of the below

**B.** REST

**C.** LDAP

**D.** SAML 2.0

**E.** Database

**ANSWER: D**

**Explanation:**

**SAML 2.0** is the supported authentication mechanism in this context because Saviynt can use Security Assertion Markup Language version 2.0 for federated sign-on. With this model, an external identity provider authenticates the user and sends Saviynt a signed SAML assertion containing the identity and relevant authentication information. Saviynt then validates the assertion and establishes the user session. This supports centralized authentication, reduces the need to maintain separate application passwords, and enables organizations to apply their existing identity-provider controls, such as multifactor authentication and conditional-access policies, before access to Saviynt is granted. Correct SAML integration requires configuring the service-provider and identity-provider metadata consistently, including entity IDs, assertion consumer service details, certificates, and expected user attributes. Saviynt's product documentation is available through the Saviynt Documentation portal. The underlying federation standard and its technical model are maintained by OASIS in the SAML 2.0 standard resources.

## QUESTION NO: 5

John, who recently joined an organization as a full-time employee, is required to work from the Sydney office. He was assigned birthright entitlements as part of the new joiner provisioning. Which of the following Enterprise Roles will be assigned to John from the Birthright Rule?

**A.** Birthright - Sydney

**B.** Birthright - Permanent - Full-time

**C.** Birthright - All

**D.** Birthright - Employee

**E.** Cannot be determined from the information provided.

**ANSWER: E**

**Explanation:**

Cannot be determined from the information provided is correct because Saviynt does not select one Enterprise Role merely by choosing the most specific-looking role name. A Birthright Rule is configured by the organization with defined user-attribute criteria and one or more access assignments, such as Enterprise Roles. During provisioning, Saviynt evaluates the configured rules against John's actual identity attributes and assigns the roles associated with every applicable rule, subject to the organization's rule configuration and any applicable lifecycle or provisioning settings.

The scenario establishes that John is a full-time employee working from Sydney, but it does not provide the Birthright Rule definitions, the attributes they evaluate, or the Enterprise Roles attached to them. In particular, role names alone do not establish whether a rule applies; a role named "Birthright - All," "Birthright - Employee," or "Birthright - Sydney" could be attached to a rule with any configured condition. Therefore, the information given cannot reliably identify a specific Enterprise Role assignment. The required configuration should be reviewed in Saviynt's birthright-rule and Enterprise Role setup. Refer to the Saviynt Documentation portal and Saviynt's Identity Governance Administration overview for product documentation and configuration context.

## QUESTION NO: 6

The process of Attestation or Certification can be best described as:

**A.** Segregation of Duties

**B.** Access Reviews

**C.** Access Request

**D.** Application Onboarding

**ANSWER: B**

**Explanation:**

Access Reviews is the best description of attestation or certification in Saviynt Identity Governance and Administration. An access review is a governed, time-bound process in which designated reviewers—such as managers, application owners, or role owners—evaluate users' existing accounts, entitlements, roles, and access-risk information. The reviewer attests that access remains appropriate for the user's job responsibilities and business need, or takes action to remove, revoke, or modify access that is no longer justified. This provides organizations with a repeatable control for validating least-privilege access and producing an audit trail of review decisions, comments, dates, and remediation activity.

In Saviynt, these reviews are commonly conducted through campaigns, which route review items to the appropriate certifiers and track completion. Certification therefore represents the reviewer's formal decision within the broader access-review process, rather than a separate access lifecycle activity. The terminology aligns with identity-governance practice: access certifications help organizations periodically demonstrate that access has been reviewed and remains authorized. Saviynt describes its IGA platform as providing access governance capabilities, including access certifications and compliance controls. See Saviynt Identity Governance and Administration and Saviynt resources for product and identity-governance materials.

## QUESTION NO: 7

Which of the following Role types should be selected for a Role containing Entitlements that span across multiple applications?

**A.** Application Role

**B.** Transactional Role

**C.** Enabler Role

**D.** Enterprise Role

**ANSWER: D**

**Explanation:**

Enterprise Role is the appropriate role type when the role must contain entitlements from more than one application. In Saviynt's role model, an enterprise role represents a business-level access package, such as a job function, department responsibility, or organizational persona. Because that business responsibility can require access in several target systems, the enterprise role can aggregate the associated application roles and/or entitlement access across those systems into one governable role assignment. This lets an organization request, certify, provision, and report on a coherent cross-application bundle of access as a single unit.

Using an enterprise role also supports a role hierarchy: application-specific access can be modeled at the application level, then combined into an enterprise role that expresses the broader business need. This separation makes role design more maintainable while preserving a clear connection between business roles and the technical access they deliver. Saviynt describes enterprise roles as the role category used to group access across applications in its role-management and training materials. See Saviynt's Identity Governance and Administration resources and the Saviynt Enterprise Identity Cloud overview.