PassQueen
a.k.a dumpsqueen.com

RSA Archer Certified Administrator 5.x Exam

RSA 050-v5x-CAARCHER01

Version Demo

Total Demo Questions: 9

Total Premium Questions: 90

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, System Integration and Configuration Management	27
Topic 2, Security Administration	14
Topic 3, Communication and Data Presentation	29
Total	90

QUESTION NO: 2

Which of the following describes what must be performed before pasting non-English text into an RSA Archer record?

A. No additional tasks need to be performed.

B. The application must be set to "Production" status.

C. The user's locale setting must match the language type.

D. The Spell Check option for the application must be disabled.

ANSWER: D

Explanation:

The Spell Check option for the application must be disabled. In RSA Archer 5.x, the application-level spell-check feature is intended to evaluate text using its configured spelling resources. Before users paste text containing non-English characters into an Archer record, the administrator should disable Spell Check for that application. This prevents the spell-check process from attempting to process pasted content in a way that may not be compatible with the text's language or character set. The setting is applied at the application level, so it should be addressed as part of the application's configuration before users enter or paste multilingual content. This is especially important for records that must retain submitted text exactly as provided, such as policy statements, assessment responses, evidence descriptions, or translated control language. Archer is an enterprise GRC platform designed to centrally manage business and risk information; application configuration choices such as text-entry behavior should therefore be validated before production use. See the Archer website for platform information and the Unicode Standard for background on multilingual character representation.

QUESTION NO: 3

What two fields are automatically added to an application when an administrator enables a workflow process? (Choose Two)

A. Workflow Stage

B. Workflow Status

C. Workflow Assignees

D. Workflow Risk Rating

E. Workflow Permissions

ANSWER: A C

Explanation:

Enabling a workflow process adds the **Workflow Stage** and **Workflow Assignees** fields to the application. Workflow Stage is the system-managed field that identifies the current point in the configured workflow path for a record. It allows the workflow engine and users to determine where the record is in its lifecycle as it moves through the defined stages. Workflow Assignees is added so Archer can maintain the users, groups, or roles responsible for acting on the record at its current workflow point. This assignment information supports routing, work queues, notifications, and accountability for workflow actions. These fields are created as workflow-supporting application fields when the workflow capability is enabled, rather than being ordinary fields that an administrator must manually define. Archer workflow configuration uses these fields to coordinate record progression and responsibility across the workflow process. See the Archer platform overview at Archer and Archer's product information for workflow-enabled integrated risk management capabilities at Archer Products.

QUESTION NO: 4

Dashboard access can be based on which of the following? (Choose three)

A. Solutions

B. Private Fields

C. Access Roles

D. Individual Users or Groups

E. Inherited Record Permissions

F. Global Report Administrator standing

ANSWER: A C D

Explanation:

Dashboard access in RSA Archer is governed through the platform's dashboard-permission model, which lets administrators make dashboards available within an appropriate solution context and then assign access to the relevant audiences. Solutions are a valid basis because dashboards are created and managed in relation to solution content and reporting assets. Access Roles are also valid because they provide the reusable, role-based entitlement mechanism used to grant users the appropriate functional access across Archer. Individual Users or Groups are valid because dashboard permissions can be targeted directly to particular users or to directory groups, enabling administrators to share a dashboard with a defined audience without creating a separate role solely for that purpose.

Using these mechanisms together supports both broad and targeted distribution: a dashboard can be placed in the needed solution area, granted to standard job-function roles, and, where required, shared with a specific user or group. This approach aligns dashboard visibility with the organization's established Archer security and access-administration model. See the RSA Archer product documentation portal at Archer Support and RSA's Archer product overview at Archer.

QUESTION NO: 5

Which of the following is NOT a required attribute for a user account?

A. User Name

B. Access Role

C. First and Last Name

D. Notification Subscriptions

ANSWER: D

Explanation:

Notification Subscriptions is the attribute that is not required when creating a user account in RSA Archer. Notifications are an optional, user- and system-configurable feature used to deliver messages about workflow assignments, record changes, questionnaire activity, and other events. A user can be created and enabled without any notification subscription being defined. Subscription settings may be configured later based on the user's responsibilities, the applications to which they have access, and the organization's communication requirements.

Keeping notification subscriptions optional is important because notification needs vary substantially among users. For example, an administrator can create an account for access, administration, reporting, or integration-related purposes without requiring that account to receive routine Archer messages. Where notifications are needed, Archer administrators can configure the appropriate delivery and subscription behavior after the account exists. This separates core identity and access setup from optional communication preferences and allows notification settings to be tailored over time.

For Archer product documentation and administrator resources, see the Archer Support portal and the Archer resources library.

QUESTION NO: 6

Which of the following is NOT a valid link type for a quick reference that appears on a workspace?

A. Report

B. Solution

C. Workspace

D. Content Record

ANSWER: C

Explanation:

Workspace is the invalid link type for a quick reference displayed on a workspace. In Archer, Quick References provide users with convenient, contextual navigation to supported objects or resources, such as reports, solutions, and content records. The Quick Reference configuration identifies the type of destination and the specific item to open, allowing workspace users to reach commonly needed information without manually navigating through menus. A workspace itself is the page container that organizes dashboards, navigation, and related user-facing content; it is not a supported Quick Reference destination type. This distinction helps keep Quick References focused on actionable or informational resources that can be opened from the workspace experience. Archer documentation and training materials describe workspace administration and navigation as separate configuration concepts from links to content and reporting resources. For product and learning information, see Archer Integrated Risk Management and the Archer resources and documentation portal.

QUESTION NO: 7

Which of the following frequencies is NOT an option for Subscription Notifications?

A. Hourly

B. Weekly

C. Monthly

D. Instantly

ANSWER: A

Explanation:

Hourly is the correct selection because Archer Subscription Notifications do not provide an hourly delivery-frequency setting. Subscription Notifications are designed to distribute saved-search or report results on the supported notification schedule choices, allowing recipients to receive recurring updates without manually running the underlying content. When configuring a subscription, the administrator or content owner selects from Archer's available delivery intervals; an hourly cadence is not one of those defined intervals. Therefore, a requirement to send subscription results every hour cannot be met by selecting a native Subscription Notification frequency and would require a different design approach, such as an integration or scheduled automation outside the standard subscription-frequency choices.

Subscription configuration is part of the Archer platform's notification and reporting capabilities. Consult the Archer product documentation portal for the version-specific Subscription Notifications configuration details and available scheduling settings: Archer Help. Additional product and platform information is available from Archer.

QUESTION NO: 8

Which of the following statements about the system administrator role is NOT true?

A. The system administrator role can be altered.

B. The system administrator role cannot be deleted.

C. Only system administrators can assign other users the system administrator role.

D. System administrators have authority to revoke application ownership for any user.

ANSWER: A

Explanation:

The statement **"The system administrator role can be altered."** is not true. In Archer, the System Administrator role is a protected, predefined system role rather than a role whose definition, permissions, or core configuration can be edited like a custom role. Archer protects this role because it provides the platform-level administrative authority needed to manage essential security and administrative functions. Keeping the role fixed establishes a dependable administrative control point and prevents a configuration change from accidentally reducing or changing the privileges required to administer the instance. Organizations can manage who is assigned to the protected role in accordance with their governance process, but they do not alter the role itself. This distinction is important when designing Archer access controls: custom roles should be created for delegated administrative or business responsibilities, while the System Administrator role remains reserved for the highest level of platform administration. Archer's official product information describes the platform's governance and access-control capabilities at Archer; implementation guidance and product resources are available through the Archer Community.