

SAP C_SEC

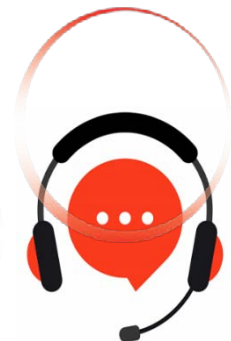
SAP Certified - Security Administrator

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/c-sec>

Latest Version: 4.1

1. Unified Scenario Simulation
2. Micro Skill Drill Exam

Topic: 1

Unified Scenario Simulation

Meridian Specialty Chemicals Secures a Two-Edition SAP Rollout

Business Context

Meridian Specialty Chemicals is a multinational group that manufactures coatings, adhesives, and industrial additives across plants in Europe, North America, and Southeast Asia. After years on a heavily customized legacy platform, the group is consolidating its manufacturing and finance core onto SAP S/4HANA in its Private Edition, while a recently acquired consumer-coatings subsidiary runs on SAP S/4HANA Cloud, Public Edition. A small central security team, expanded for the programme, owns access design and administration for both. Go-live for the first wave is weeks away, and the team is part-way through a cutover rehearsal before hypercare begins.

System Landscape

The landscape brings together the Private Edition core, the cloud subsidiary, a HANA Cloud environment that serves group-wide analytics, and a Fiori launchpad that most business users will use as their entry point. Authentication for the cloud services is being centralized through SAP Cloud Identity Services, with identities meant to flow from the group's authoritative human-resources record. For the on-premise core the team maintains development, quality, and production systems, and moves authorization changes between them along the formal transport path.

Role Design Context

The security lead wants one coherent business-role concept the auditors can follow, even though the two editions express access differently. In the Private Edition core, access rests on the classic concept of authorization objects, roles, and the profiles those roles generate; in the cloud subsidiary, access is expressed through business roles built from business catalogs. Front-desk and plant-floor staff perform the same job at many sites yet must each be confined to their own plant. During rehearsal, several plant clerks in the core can open their task screens but are stopped the moment they try to post.

Launchpad Observations

Many users reach their Fiori launchpad and see their tiles, yet a recurring rehearsal report is that certain apps open to an empty screen or an authorization message the instant they request data. The apps that fail are not the same across user groups, and a few power users see everything while their teammates see nothing. The team has been adding catalogs in response, with mixed results, and is unsure why the pattern varies.

Identity Integration

The cloud subsidiary's users are meant to sign in through the central identity service and be provisioned into the connected applications automatically as the human-resources record captures them. In rehearsal, a batch of new joiners could authenticate but were not recognized by one target application, while several leavers recorded as departed were found still able to sign in. To keep the rehearsal moving, the team had created some accounts directly in the target applications, outside the central flow.

Analytics Governance

Group analytics run on HANA Cloud, where a set of analysts build their own reports over shared schemas. A rehearsal review found that one analyst's report surfaced personally identifiable customer fields her role was never meant to include; her access had been granted at a broad level so her general

reports would work. Separately, finance wants month-end reporting to run fast, and one proposal on the table is to widen analyst access broadly so that no mid-close access request can hold up reporting.

Governance Pressure

The group's auditors expect access to match current responsibilities, sensitive duties to stay separated, and a clear trail of who can do what. The rehearsal has exposed both under-provisioned users who cannot complete their tasks and over-provisioned users who can reach more than they should. The team is conscious that go-live will multiply both patterns across thousands of users if the underlying concept is not settled now rather than patched case by case.

Close Preparation

With the rehearsal window closing, the team must settle the role concept across both editions, reconcile the launchpad behavior, stabilize the identity flows, and bring analytics access within policy — while keeping the two editions consistent enough to tell one audit story. The decisions taken this week will carry directly into hypercare.

Your assignment

You are a member of Meridian Specialty Chemicals' central security team during the cutover rehearsal for the first go-live wave. You work across an SAP S/4HANA Private Edition core, an SAP S/4HANA Cloud, Public Edition subsidiary, a HANA Cloud analytics environment, a Fiori launchpad, and SAP Cloud Identity Services. Your task is to settle the access concept and resolve the anomalies surfaced in rehearsal so that, at go-live, users can perform exactly their own responsibilities and no more, consistently across both editions, with access changes that move correctly through the landscape

1. CHALLENGE 1 — Designing One Business-Role Concept Across Two SAP Editions

- Establish the plant-clerk access in the Private Edition core so it grants the activities the job actually performs, including posting, not only display.
- Build the role structure so identical capabilities apply at every plant while each clerk is confined to their own plant's organizational values, and the design remains maintainable as it changes.
- Express the equivalent access in the cloud subsidiary using its own access model rather than transplanting the classic model.
- Ensure authorization changes prepared in the quality system become effective in production through the landscape's transport path.

Checkpoints

- A plant clerk can both open and post in their transactions, confined to their own plant.
- A change made once to shared authorizations is reflected for every plant without per-plant rework.
- A user in the subsidiary receives job-appropriate access expressed in that edition's model.
- A change validated in quality is present and effective in production.

2. CHALLENGE 2 — Aligning Fiori Launchpad Tiles With Backend Data Authorizations

- Distinguish the access that places an app on the launchpad from the access that authorizes the data and actions the app performs.
- For apps that open but return no data, identify and grant the missing backend authorization rather than re-adding frontend content.
- Use an authorization trace on a failing user to pinpoint the specific missing authorization before changing roles.
- Bring over-provisioned users back within the scope their responsibilities require rather than using them as a template.

Checkpoints

- A representative user opens an app and it returns their permitted data.
- A failing app is resolved by a backend authorization change traceable to evidence, not by broad additions.
- Power users hold only the access their responsibilities require.

Question: 1

CHALLENGE 1 — Designing One Business-Role Concept Across Two SAP Editions

During rehearsal in the Private Edition core, several plant clerks can open their task screens but receive an authorization error the moment they try to post.

The clerks can display the relevant transactions but cannot post. What is the most likely cause and the correct corrective action?

- A. The role does not grant the underlying function at all; re-add the function so the clerks can both open and post in the transaction.
- B. The role authorizes display but not posting; add the posting activity to the relevant authorization.
- C. A change enabling posting was made but never transported; re-open and re-test that change in the quality system.
- D. The clerks need broader plant-operations access; assign them a wide operations role so posting is no longer blocked.

Answer: B

Explanation:

Opening the screen proves the function is assigned, so the gap is at the activity level — the authorization permits display but not posting. Adding the posting activity to that authorization grants exactly what is missing while keeping the clerks least-privileged. They can then post without any widening of their access.

Question: 2

CHALLENGE 1 — Designing One Business-Role Concept Across Two SAP Editions

The same plant-clerk job exists at many plants, and each clerk must be confined to their own plant's data while all plants receive identical capabilities.

How should the team build the plant-clerk role so capabilities are identical, each clerk is confined to their own plant, and the design stays maintainable?

- A. Build a master role with the common authorizations and a derived role per plant for its organizational values.
- B. Copy a finished plant-clerk role once per plant and edit each copy to point at its own plant.
- C. Build one plant-clerk role covering all plants, assigned to everyone, relying on staff to open only their own plant.
- D. Build the common role once and set each clerk's plant values directly on the user record, outside the role.

Answer: A

Explanation:

A master role holding the shared authorizations with a derived role per plant lets the common part be maintained once and flow to every plant, while each derived role confines its clerks through that plant's organizational values. Changes propagate consistently, and the structure is auditable. It satisfies both confinement and maintainability.

Question: 3

CHALLENGE 1 — Designing One Business-Role Concept Across Two SAP Editions

In the S/4HANA Cloud, Public Edition subsidiary, access is expressed differently from the Private Edition core, and the team must grant a job's access in a way the auditors can follow.

How should the team grant a subsidiary user the access their job requires?

- A. Generate profiles from authorization objects and assign those profiles to the user, exactly as in the core.
- B. Grant the user database-layer privileges directly so the applications they use will accept them.
- C. Assign the appropriate business role or roles, built from business catalogs, to the business user.
- D. Maintain the individual authorizations directly on each user without using any role.

Answer: C

Explanation:

In the cloud edition, access is governed by the business user concept, where business roles built from business catalogs carry the access. Assigning the appropriate business roles gives the user job-appropriate access in that edition's own model and keeps the design auditable. It is the construct that edition expects.

Question: 4

CHALLENGE 2 — Aligning Fiori Launchpad Tiles With Backend Data Authorizations

Several users reach their launchpad and see their tiles, but certain apps open to an empty screen or an authorization message the moment they request data.

What is the most likely cause of apps opening but returning no data, and the correct action?

- A. The users are missing the catalog that places the tiles; re-assign the catalog so the apps can load their data.
- B. The users can reach the apps but lack the data authorization behind them; grant the backend authorization.
- C. The launchpad content is stale for these users; have them clear the launchpad cache and reopen the apps.
- D. The users need a wider launchpad role so the apps receive whatever data they request when opened.

Answer: B

Explanation:

The users can reach the apps but lack the data authorization behind them; grant the backend X
The tiles appear and the apps open, so frontend access is in place; the refusal at the point of requesting data indicates the backend data authorization is missing. Granting that backend authorization lets the apps return the user's permitted data. The fix is at the layer that is actually being refused.

Question: 5

CHALLENGE 2 — Aligning Fiori Launchpad Tiles With Backend Data Authorizations

The apps that fail differ across user groups, and a few power users see everything while their teammates see nothing.

What is the best first action to pinpoint why specific apps fail for specific users?

- A. Trace a failing user reproducing the error to find the missing authorization.
- B. Assign every available catalog to the failing users so that no app can be missing its access.
- C. Copy a power user's role to the failing users so they immediately gain the same access.
- D. Rebuild the launchpad content for the failing groups so the apps are presented to them again.

Answer: A

Explanation:

A trace taken while a failing user reproduces the error shows exactly which authorization is being refused, letting the team grant the specific missing backend authorization. It pinpoints the cause before any role change and keeps the correction minimal. Evidence drives the fix.

Question: 6

CHALLENGE 2 — Aligning Fiori Launchpad Tiles With Backend Data Authorizations

Investigation shows the power users can reach far more data than their roles were ever meant to allow. Given the auditors' expectation that access match responsibilities, what should the team do about the over-provisioned power users?

- A. Leave their access unchanged, since power users are expected to see more than their teammates anyway.
- B. Use their broad access as the template for everyone so all users can see everything the apps offer.
- C. Reduce their access to only what their responsibilities require.
- D. Add a restrictive role on top of their existing access to exclude the data they should not reach.

Answer: C

Explanation:

The auditors require access to match responsibilities, so the over-provisioned access must be reduced to what each power user's role actually needs. Removing the excess backend authorizations brings them within least privilege without affecting their legitimate work. It corrects the over-grant at its source.

Question: 7

CHALLENGE 2 — Aligning Fiori Launchpad Tiles With Backend Data Authorizations

The team has been adding catalogs in response to the data errors, with mixed results. Why does adding more catalogs fail to reliably resolve apps that return no data?

- A. The catalogs must be added in a specific sequence, and the additions failed because the order was wrong.
- B. Catalogs add tiles (frontend), but the failures are missing backend data authorizations, not tiles.
- C. The catalogs were created in the wrong system and must be transported before they take effect.
- D. The catalogs conflict with one another, so each new catalog cancels the data access granted by the last.

Answer: B

Explanation:

Catalogs govern the frontend — which apps a user can reach — whereas the empty-screen failures are refusals at the backend data layer. Adding catalogs therefore adds or confirms tiles without granting the data authorization the apps actually need, which is why results are mixed. The data layer must be addressed directly.

Topic: 2

Micro Skill Drill Exam

Question: 8

An international logistics provider runs several SAP cloud applications alongside an existing on-premise system used by its inland depots. Today employees keep separate passwords for each of the cloud apps, help-desk password resets are frequent, and the security team wants people to sign in with their existing corporate identity provider so there is a single, consistent authentication experience across the hybrid landscape. Separately, the team also wants user accounts to be created and kept up to date automatically in the cloud applications as people join, move between depots, or change roles, so that account data does not drift. The administrator is reviewing SAP Cloud Identity Services, which provides one capability focused on authenticating users and another focused on provisioning and synchronizing accounts, and must decide which capability addresses the single sign-on requirement specifically rather than the account-lifecycle requirement.

Which SAP Cloud Identity Services capability should the administrator configure to enable single sign-on through the corporate identity provider?

- A. The Identity Provisioning Service, because it creates and synchronizes the user accounts that the cloud applications depend on for access.
- B. A combined HANA privilege role, because database-level roles are what control how users are allowed to sign in to cloud applications.
- C. The launchpad business catalog, because the catalog assigned to users is what determines whether they are permitted to authenticate to the apps.

D. The Identity Authentication Service, configured to delegate authentication to the corporate identity provider so users get single sign-on.

Answer: D

Explanation:

The Identity Authentication Service is the SAP Cloud Identity Services capability dedicated to authentication. Configuring it to delegate authentication to the company's corporate identity provider gives employees one sign-in across the cloud apps, which is exactly the single sign-on outcome described. It targets the authentication requirement directly and leaves provisioning to the separate service.

Question: 9

A security administrator at a regional water utility supports an on-premise SAP S/4HANA system. A meter-reading clerk was recently moved from the billing team to the field-operations team. After the move, the clerk can still open the billing transactions she used before, but reports being blocked when running a field work-order display, where she receives an authorization error. The administrator confirms the clerk's user record is active and that the field-operations role already exists and is correctly built with the authorizations the work-order display needs. Looking at the user record, the administrator sees that only the billing role is still assigned — the field-operations role was never added when the clerk changed teams. Company policy requires least-privilege access and the removal of access that a user no longer needs in a new position.

What is the correct action to restore the clerk's required access while honoring company policy?

- A. Reset the clerk's user record and recreate it under the field-operations team so that the earlier billing assignment is cleared automatically.
- B. Rebuild the field-operations role so it also contains the billing authorizations, then leave both capabilities active under that single role.
- C. Add a wide reference authorization that grants display access across all operational areas, so the clerk is not blocked again after any future team move.
- D. Assign the existing field-operations role to the clerk's user record and remove the billing role that is no longer needed in her new position.

Answer: D

Explanation:

The field-operations role already carries exactly the authorizations the work-order display checks, and the user record is active, so the only gap is that the role was never assigned during the team change. Assigning that role grants precisely the access the new position needs, and removing the now-unneeded billing role keeps the user within least-privilege and reflects the change of duties. This matches both the trace finding and company policy.

Question: 10

A new accounts-payable associate joins a specialty retail chain that runs SAP S/4HANA Cloud, Public Edition, across its store-support and finance back office. On her first day the security administrator must give her access to the supplier-invoice processing apps so she can begin clearing an invoice backlog. In this edition, access is governed by the business user concept: a business role bundles the business catalogs that expose the apps a user is allowed to open, and the business role is then assigned to the business user. The administrator has already created the business user for the associate, but is unsure how to grant the app access so that the correct apps appear on her launchpad and she can process supplier invoices. Other accounts-payable colleagues already work with these apps every day without issue, so the required access set is well understood, and the team wants the new associate provisioned the same consistent way rather than through a one-off arrangement. What is the correct way to provide the associate the required app access?

- A. Assign a business role that contains the business catalogs for supplier-invoice processing to the associate's newly created business user.
- B. Add the individual supplier-invoice apps directly to the associate's business user, bypassing any business role so access is granted faster.
- C. Grant the associate the administrator business role for now so the apps appear, and plan to narrow the access down to what she needs later.
- D. Create a new business catalog for the associate and place her business user inside that catalog so the supplier-invoice apps become visible.

Answer: A

Explanation:

In SAP S/4HANA Cloud, Public Edition, the business role is the construct that carries business catalogs, and assigning that role to the business user is what exposes the bundled apps on the launchpad. Because colleagues already use these apps, a business role with the supplier-invoice catalogs exists or can be built from that pattern. Assigning it grants exactly the intended apps and keeps the access maintainable and consistent across the team.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>