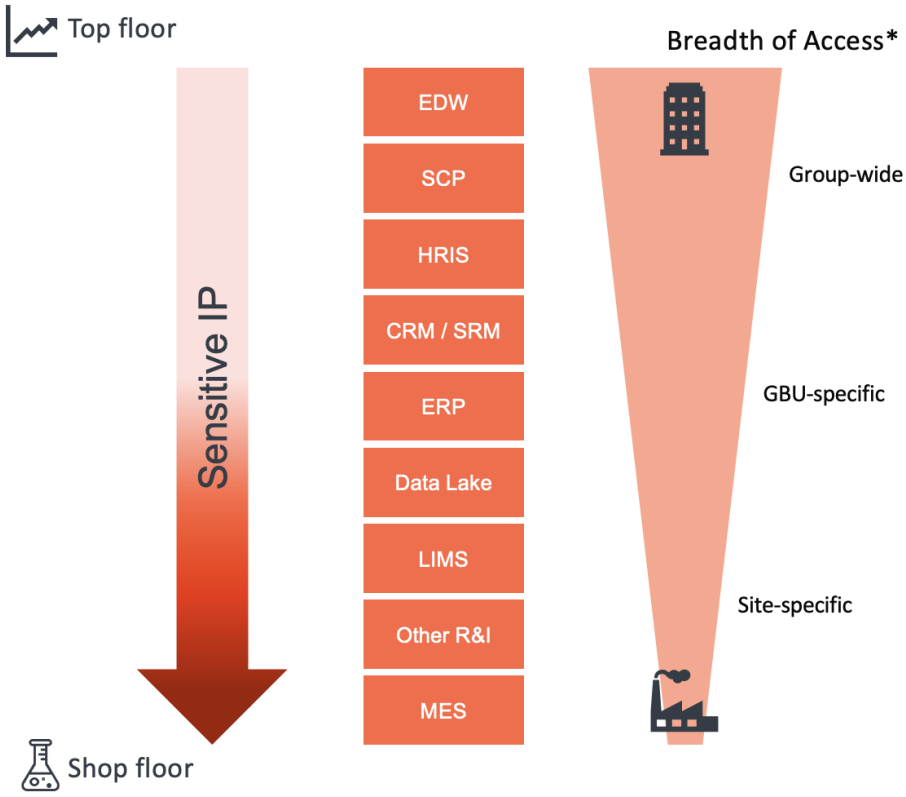
Security Approach

This document describes the overall approach to security and authorisations taken by the ERP Rebuild program across the applications and processes in its scope. It defines a number of general security aims and objectives, and the principles and specific design choices made to ensure these aims are realised by the project. The subsequent Detailed Design phase of the project will further expand on the level of detail in many areas, such as authorisation role design, specific Segregation of Duties rules, etc. in line with the principles and approaches described here.

General Security Approach

The diagram in this section aims to visually describe the general approach taken by the ERP Rebuild security design.



Sensitive IP tends to be concentrated in R&I and Manufacturing

As an innovation-driven, science-based company which manufactures many proprietary and highly-specialised products, the sensitive intellectual property of Syensqo is more concentrated in IT systems at or near to the "shop floor", as compared to enterprise systems such as CRM, Supply Chain Planning, or even ERP. Sensitive IP includes proprietary data about Syensqo's products and their design, formulation, composition, and manufacture, but also information about the design and configuration of the manufacturing processes themselves. Loss of such information could benefit Syensqo's competition and erode the company's market position, and thus this must be closely guarded.

Enterprise Systems hold comparatively less Sensitive IP

Enterprise systems farther removed from the research and manufacturing operations may of course contain data which must be safeguarded against improper access or loss, such as financial data or personal information, but generally contain less sensitive intellectual property than systems in the R&I and manufacturing domains. Legal and regulatory requirements may exist to mandate specific safeguards for any kind of data regardless of which systems they reside in. However sensitive IP is distinguished by the need to closely control access even in the absence of specific regulatory requirements due to the value to Syensqo.

As can be seen in the diagram, ERP systems straddle the boundary between these "top floor" and "shop floor" worlds. ERP systems contain some limited "shop floor" IP, such as bills of materials, but this is generally a small fraction of the total. Due to this limited volume, and the limited number of users and processes which must access this, targeted security controls can thus be implemented to protect it.

Access to Sensitive IP will be narrowly constrained

As a general principle, the more closely data is related to manufacturing, product development, and other "shop floor" concerns, the more restricted the access. At its most extreme, access to Bills of Material will be granted to only those users who require this for their jobs, and only to those materials extended to the locations at which those users work and their GBU. To implement the *need to know* and *least-privilege* principles, personnel with manufacturing access inside ERP will not be able to see sensitive data about materials not explicitly marked as relevant to their work locations or GBUs.

Broad access across organisation units precludes access to Sensitive IP

Users who, by virtue of their job, require access to data from multiple Plants or across GBUs, such as workers in GBS or Transversal functions, will be prevented from accessing sensitive IP altogether. Many job functions genuinely require access to data across multiple plants, countries, GBUs, or other organisation structures. However such access cannot be granted to Sensitive IP due to the risk of large-scale disclosure and loss.

The principle of least privilege continues to apply here to limit access only to the data required for the user's job. For example, a Regional Transportation Planner will have access only to their assigned region, rather than to all data globally.

Regulatory constraints are enforced at all times

Regulatory requirements such as export controls may place additional restrictions upon data access. These will be enforced using systematic controls at all times, and will act in addition to the organisational restrictions explained above.

Authorisations are determined from HR data, with exceptions

Authorisations granted to users of the systems created by ERP Rebuild is determined from HR data maintained in SuccessFactors. Only persons who exist in the organisation structure inside SuccessFactors will be issued with a logon account into any of the ERP Rebuild systems. Authorisations will be granted based on the person's job in SuccessFactors, as well as organisational assignments such as GBU, Country, and Plant. The standardisation across the business of Jobs is foreseen to happen as part of a Workforce Transition exercise conducted in support of ERP Rebuild, which will define standard jobs based on standard processes and roles, which will in turn drive access in the system.

Authorisations derived from a person's job can be extended as a result of multi-hatting (holding multiple jobs) after appropriate approval. Specific export licenses may also provide for certain users to gain access to data or organisational units beyond the usual rule-based authorisation scope. Where such licenses exist, the relevant additional authorisations are granted on a temporary basis using enabler roles. Assignment of additional authorisations as a result of multi-hatting or export licenses is always time-bound, subject to periodic re-certification, and governance in SAP Identity and Access Governance.

Data is encrypted at all times

All systems in scope of ERP Rebuild will apply encryption to data at rest and in transit. Unencrypted connections from users to systems are not permitted. Connections between systems and system components must be encrypted. At-rest encryption is applied in the manner most relevant to protect the data against disclosure.

The following sections of this document provides additional detail.

Contents

Summary of Major Design Decisions

- Access to specific sensitive data (e.g. Bills of Material, Routings, and other objects holding key Syensqo Intellectual Property) is restricted using the Sensitive Object Model and assigned to users based on the 'Need to Know' principle.
- For non-sensitive data, access is grouped by country, region, and global levels, and is assigned based on job roles in SuccessFactors.
- The Non-Sensitive Object Model supports the GBS function, allowing broader access to Finance operational data to be able to effectively support finance shared service operations.
- For export controls, the security model uses a layered approach, combining Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) using NextLabs.
- Cross-country access is granted to specific users with an Export Control License using Enabler Role.
- For reporting, authorisations are mirrored from S/4HANA to ensure data restrictions in reports.
- For authentication, a transition from InWebo to Microsoft Authenticator is recommended due to the latter app's support for geo-locating users in aid of export control enforcement.

- The Job-role mapping is maintained in GRC, with reports generated in DataSphere to combine process information and job-role mapping.
- SAP user provisioning is automated using Identity Access Governance (IAG), based on jobs assigned in SuccessFactors.
- Segregation of Duties (SoD) conflicts are addressed at the process role, job role, and user levels using the IAG tool for both on-premise and SaaS applications.
- Emergency Access Management for S/4 HANA is handled via GRC AC, and third-party tools for SaaS will be evaluated during the detailed design phase.
- Multi-hatting requests are managed through the IAG tool to grant access to users with additional responsibilities beyond their primary job roles.
- User access reviews for multi-hatting & IT Support roles are conducted semi-annually using the IAG tool, with the process requiring recertification of user access.

Authorisation Concept Summary

The table below summarises the different authorisation concepts used in systems covered by ERP Rebuild.

Application	Location	UI Entry Point	Authorisation Concept
S/4 HANA	On Premise	SAP Build Work Zone	SAP ABAP-based authorisations
GTS	On Premise	SAP Build Work Zone	SAP ABAP-based authorisations
GRC	On Premise	SAP Build Work Zone	SAP ABAP-based authorisations
SuccessFactors	Cloud	SAP Build Work Zone	SuccessFactors RBP (Role-Based Permissions)
Ariba	Cloud	SAP Build Work Zone	RBP, using *Custom Groups*
SAC	Cloud	SAP Build Work Zone	RBP, using *Teams*
Datasphere	Cloud	SAP Build Work Zone	RBP, using *Scoped Roles*

Authorisations in S/4HANA

Sensitive Objects

The following information is considered to be sensitive and thus protected using fine-grained authorisations which strongly limit access:

- Bills of Material, including Costing BOM
- Routings
- Recipes
- Processing Instructions
- Certain lab analysis results
- Product compositions in the Product Compliance module
- Detailed margin (selling product and customer) information for Specialty Polymers
- Certain R&I projects explicitly considered to be sensitive
- Group-level financial results

Roles associated with sensitive objects are crucial for preventing unauthorized access. For areas where data needs to be more secure, custom authorization objects can be employed to meet business requirements. Consequently, these roles will be defined at the lowest level required by business needs and assigned carefully according to the **'Need to Know'** principle.

The GBU organization is structured into Commercial and Operational segments. The Sales Org represents the commercial side (e.g., one commercial GBU cannot view another GBU). On the operational side, some plants located abroad are owned by company code located in another country (e.g., Plant in Germany is owned by the Company in Belgium). To implement the security principles outlined in this document with plants abroad, an enabler role concept is leveraged.

Restrictions are required for the following modules/streams to protect GBU Commercial / Operational data:

- **Finance**: Company Code, Segments (Operating), Profit Centre Hierarchy, Profit Centre Group
- **Sales**: Sales Organisation
- **Projects**: Profit Centre Hierarchy, Profit Centre Group
- **Procurement / Ariba:** Company Code, Purchase Organisation
- **Supply Chain :** Plant, Warehouse Number

Restrictions can be applied at either the organisational level or the authorisation object level. To simplify derivation and maintenance and to avoid a large number of enabler roles, authorisation object-level restrictions can be elevated to the organisational level. Cost Center Hierarchy, Profit Center Hierarchy, and Segments, which are initially at the authorisation object level, can be converted to organisational levels when necessary.

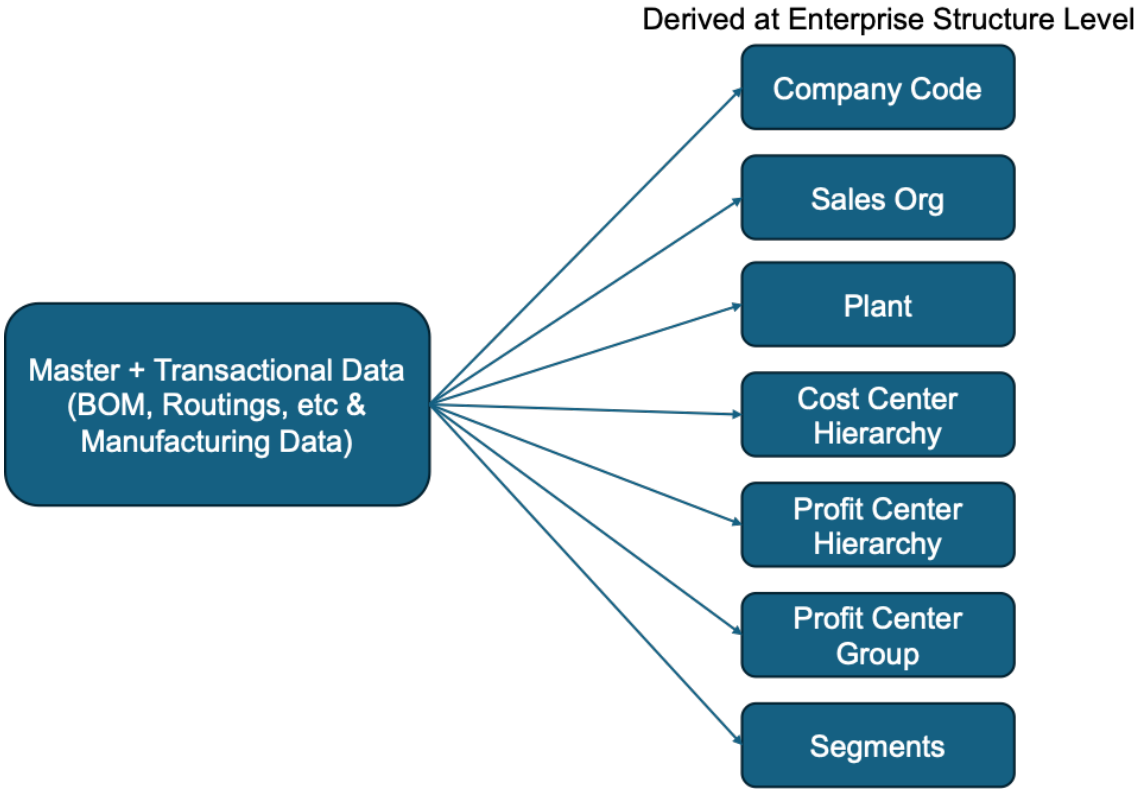
For PPM, the Access Control List (ACL) will be implemented to provide an additional layer of security, restricting to specific portfolios or projects.

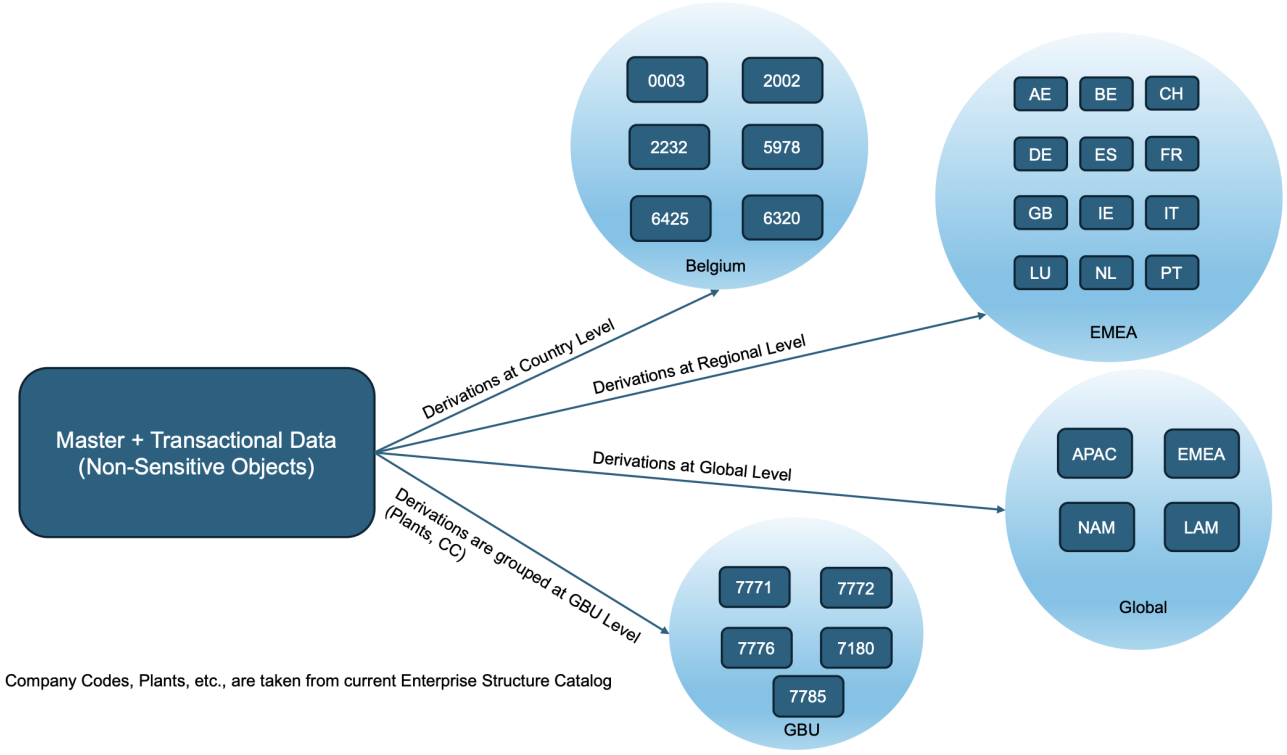
With the relocation of the in-house banking solution into the core S/4 HANA system and the potential re-integration of the in-house bank reporting entity into its respective legal entity (e.g. reporting entity '2232' from PI1 may be merged with its parent legal entity '2002' in S/4 HANA) , special requirements may arise on how access can be restricted appropriately in the affected entities given the heightened sensitivity of the in-house bank transactional data.

Non-Sensitive Objects

For users whose job does not involve sensitive objects, the following non-sensitive roles are ***broadly*** assigned and grouped for Security Purposes:

- Company Codes, Sales Organizations, and Plants are grouped by **Country**
- Countries are grouped by **Geographical Regions**
- Regions are grouped at the **Global level**





Company Codes, Plants, etc., are taken from current Enterprise Structure Catalog

As illustrated above, the company codes in Belgium are grouped together under a 'Country' derivation, meaning that all company codes for that country are included within a single role. This grouping approach is applied to all organizational elements, such as Sales Org, Purchase Org, and Plants, aligning them at the company code level within each role.

For regional role derivation, all countries within a specific geographical region are grouped together, and the relevant organizational elements are included within a single role to create a regional role.

In the case of Global Role Derivation, all regional roles are combined to form a global role. This methodology streamlines the role library, making it easier to manage and maintain roles efficiently over time.

Role derivations are also grouped by GBU's plants (as illustrated above with 'Composite Materials' GBU plants) based on business needs.

Some Finance jobs have global responsibilities, requiring broad access to support Finance functions such as GBS. These jobs do not have access to sensitive IPs but are limited to operational data such as invoice, POs etc., from relavent processes executed by the respective departments to be able to effectively support finance shared service operations. Adhering to the above model, Finance GBS will therefore be considered a global entity on its own with global access rights. However, group-wide financial results are treated sensitively and will only be accessible to authorised user groups.

Due to high data sensitivity of the global business unit 'Specialty Polymers' up to the contribution margin level, special access rights may need to be granted to safeguard the confidentiality of the recorded data in the system. As such, it may be managed separately under a Sensitive Object Model which will be further assessed during detailed design.

Transportation Management (TM)

Transportation Management (TM) requires broader access for effective operational planning and cost savings, necessitating access across multiple GBUs, which is an exception to our standard in-country, regional, global or access grouped within their GBU. Since TM does not involve viewing or accessing sensitive data, this broader access aligns with our principle of supporting business needs. Additionally, TM-specific authorizations will be restricted based on business requirements, providing an extra layer of security for users in line with the outlined principles.

Role Design

Display Roles are essential and an integral part of processes. Therefore, process-specific and cross-process display roles must be modeled in SAP Signavio, as they will be utilised by both their own and other processes for daily tasks (e.g., a Finance user may need access to display PR/POs).

Master & Derived Roles are key concepts in SAP's role-based access control (RBAC) framework, used to manage and streamline user authorizations across the SAP landscape. A **Master Role**, also known as a Parent Role, is a template role that contains the core set of authorization objects and permissions required for a specific business function. It serves as the foundation for creating multiple derived roles. A **Derived Role**, also known as a Child Role, is created based on the Master Role but with specific variations tailored to different organisational units. While it inherits the core authorizations from the Master Role, it can have different organizational level values (e.g., company code, plant, sales area) to reflect the specific needs of each unit.

Master and derived role methodologies are adopted to support both sensitive and non-sensitive object models, ensuring the requirements are met in line with the principles outlined above. Derived roles from various processes are aggregated to form composite role (Job) and assigned to users through the job-to-role mapping exercise, while master roles are never directly assigned to users.

Syensqo's security requirements for compartmentalisation and the implementation of the Need to Know Principle further require the use of Enabler Roles, in addition to Master/Derived Roles. The **Enabler Role** concept is a strategic approach in SAP security and authorisation management that involves creating roles with specific permissions designed to enable or facilitate certain functions within the SAP system. These roles are typically used in conjunction with other roles to grant additional, often temporary, access to perform specific tasks without giving full, unrestricted access to sensitive functions.

Key Aspects of the SAP Enabler Role Concept:

- **Purpose-Specific Access:** Enabler roles are designed to provide access to specific functionalities or objects that are not typically included in a user's standard role. This ensures that users only receive the permissions necessary for specific tasks.
- **Layered Authorization:** Enabler roles work in conjunction with other roles, adding a layer of access without modifying the core roles assigned to a user. This layered approach helps maintain the principle of least privilege while still enabling the necessary functionality.

The Enabler Role will be adopted and used exclusively for GBU Operational purposes & Export Control License, such as when an extension to a company code, plant, etc., or cross-country access is needed to carry out business operations. This concept will be deployed to enable regular exceptions to the country- or GBU-based authorisation model. The 'Plant Abroad' model is a good example of the use of Enabler Roles: Typically a user in Belgium with a job whose access is delimited by country (i.e. restricted to Belgium) must also be able to interact with a Plant Abroad which belongs to a Belgian entity, but is physically located in Germany. To realise this, an Enabler Role will add authorisations scoped specifically to only the Plant Code of the German Plant to the role which provides access to Belgian plants.

The Enabler role will also be utilized for 'Export Control License' granted to select users who require cross-country access to perform operations. This role is assigned alongside the user's primary job role, providing cross-country access without affecting their regular job responsibilities.

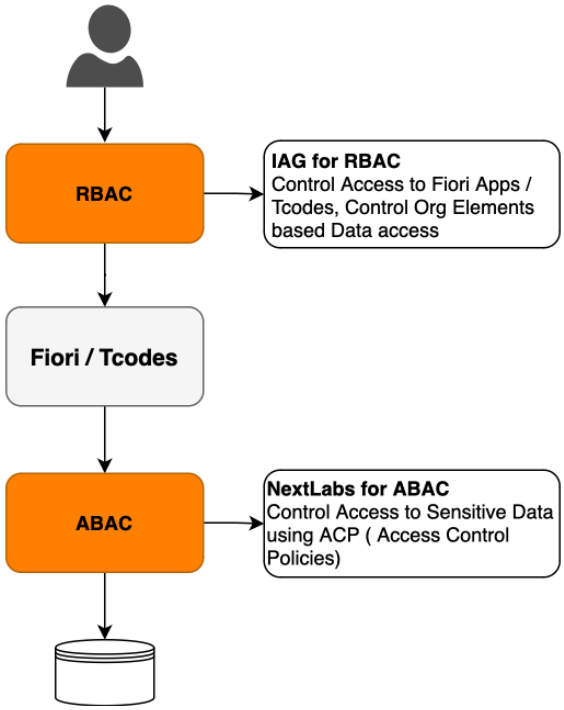
For ITAR Export Controls, the security model employs a hybrid approach that integrates Role-Based Access Control (**RBAC**) and Attribute-Based Access Control (**ABAC**), using NextLabs products to protect global data access. The implementation of this mechanism is described in Confluence in more detail.

Layering Role-Based and Attribute-Based Security

Access to sensitive data is managed through a combination of RBAC and ABAC, using respective tools: IAG for RBAC and NextLabs for ABAC, to safeguard global data access. User access is initially verified by the RBAC framework, where data is restricted through organisational elements and authorisation checks. NextLabs Data Access Enforcer (DAE) product enforces Access Control Policies to regulate access to sensitive information. Users go through multiple levels of defence before accessing sensitive data:

- **Level 1:** Need to know, exceptions granted via licenses.
- **Level 2:** Person Attribute based check

The information for Level 2, including nationality, physical location, and employment status, is retrieved from SuccessFactors and integrated into NextLabs. The details of the interface mechanism, including whether the Access flag tool will remain part of this process, will be determined during the detailed design phase.

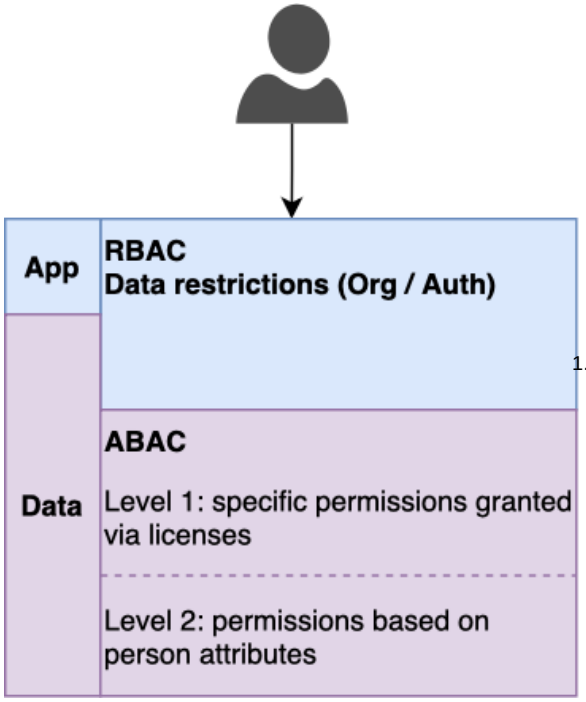


SAP-standard Role-Based Access Controls (RBAC) are used to control access to Fiori apps, Transactions, etc. as per good practices for SAP implementations. However this approach is limited to the authorisation objects delivered by SAP, and may not deliver a result that is fine-grained enough to satisfy the security objectives of Syensqo for the protection of Intellectual Property or compliance with export controls.

This approach is thus supplemented by Attribute-Based Access Controls (ABAC), implemented by NextLabs. This allows authorisation decisions to be made using a far greater number of attributes of a user and their current session with the system, including transitory attributes such as the geographical location of the user.

The implementation of ABAC bring with it certain administrative overheads in the development of attribute-based control policies, and potential performance overheads. Thus ABAC should only be used where necessary.

Implementing ABAC as a second layer of authorisation checks means that most authorisation decisions can be made by standard SAP RBAC, and ABAC is only used where access must be further delineated. This will help to minimise the absolute number of ABAC checks performed at runtime.



ABAC checks themselves will be implemented in two layers:

1. Specific permissions assigned to the user are checked first. Specific export licenses may exist to permit certain users access to information which they would otherwise be prohibited from accessing. This first layer thus allows licenses such as Technical Assistance Agreements to be enforced by the system.
2. If no specific permissions exist, access decisions are then made using other attributes of the user, such as citizenship status, geographical location, etc.

Authorisation Object Maintenance

SAP delivers predefined authorization object data, which consists of relevant authorization objects for each application or system entry point, such as Web Dynpro applications, OData services, and more.

If, during detailed design, it is discovered that standard SAP-delivered authorisation checks are insufficient for certain transactions, then the authorisations are extensible using custom authorisation objects and checks.

Any custom developments must include Authorization Object checks in order to ensure these custom developments can implement the security approach described in this document.

Project Role Design

During the project phase, the project team requires access to explore and work with new functionalities delivered by SAP through its latest releases. To enable this, while maintaining appropriate access controls and avoiding excessive privileges between teams - S/4HANA project roles have been thoughtfully designed and segmented into six distinct categories. Each role is tailored to meet the specific requirements of different project teams.

The defined roles are:

1. **Project Functional Role**

   Includes all necessary transaction codes and apps for the functional teams to perform their tasks, such as configuration and data setup. Access is limited to functional activities and excludes Development, Security, and Basis-related transactions.
2. **Project Technical Role**

   Focused on development and integration work, this role includes only the technical transaction codes and apps needed by the technical team. It does not include access to Security or Basis administration functions.
3. **Basis Admin Role**

   Contains all system-related transaction codes and apps required by the Basis team to perform system administration tasks. It provides full access relevant to Basis operations.
4. **Security Admin Role**

   Includes only security-related transaction codes and is assigned exclusively to the Security team for managing user access, roles, and authorisations.
5. **System & Communication Role**

   Includes transaction codes and access required for configuring system integrations, managing communication interfaces, and setting up background jobs for both internal and external systems.
6. **Broader Display Role**

   This role is intended for users who require read-only access across various functional and technical areas. It enables comprehensive visibility into system data, configurations, and processes without granting any change or configuration permissions. It is typically assigned to stakeholders, auditors, or team members who need to review system information without making modifications.

These roles are assigned to the appropriate teams once the development systems are available, with access restricted based on role requirements.

Support Role Design

In the post-go-live phase, the Sy-way Support team plays a critical role in maintaining system stability, ensuring smooth business operations, and addressing day-to-day issues. To facilitate this, a structured **Support Role Design** has been implemented, aligned by **business process areas** and with a strong focus on **security, compliance, and Segregation of Duties (SoD)**.

Support roles are categorized based on key business process streams to ensure focused access and accountability. These include:

1. Idea to Market (I2M)
2. Source to Pay (S2P)
3. Plan to Fulfil (P2F)
4. Lead to Cash (L2C)
5. Acquire to Decommission (A2D)
6. Record to Report (R2R)
7. Budget to Forecast (B2F)
8. Safety to Sustainability (S2S)
9. Hire to Retire (H2R)

Each role is:

- **Strictly limited to the transaction codes and Fiori apps required for daily support activities** within that process area.
- **Designed to be free from SoD conflicts**, ensuring clean role assignments and reduced audit risk.
- **Built with the principle of least privilege**, granting only the necessary access required for routing issue resolution, data validation, and configuration review.

To maintain security and compliance, any access **outside the scope of the assigned support role** must follow a controlled elevation process:

- Users requiring temporary access to perform activities not covered by their standard support roles must follow the **Emergency Access Management (EAM)** process.
- This involves **raising a request**, obtaining the required **approvals**, and **using a Firefighter ID** or equivalent mechanism to perform elevated tasks.
- **All elevated access is logged and auditable**, with post-usage review and monitoring in place.

SAP Build Work Zone

Build Work Zone will serve as the entry point for all users at Syensqo. For detailed information, refer to the KDD User Access to Enterprise Systems do cumentation.

Role Design Standards for All Applications in Scope:

- Roles will be derived from SAP Signavio process models.
- Spaces, Pages and section definitions will follow the L2, L3, and L4 information from SAP Signavio.
- Swimlanes will be aggregated to form Composite Roles based on their Job-Role mapping.
- A Master Catalog will be created for each process.
- A Swimlane Catalog will be created for each role, referencing the Master Catalog.

Role Structure and Definition:

Swim lane containing Tcodes, Fiori Apps, and Reports, are extracted from SAP Signavio. Based on this information, swim lanes are structured, and definitions are created in the S/4 HANA system.

The Master Catalog contains all Fiori Apps and Transaction Codes associated with each process, with one Master Catalog created per process. If there are changes to the process, such as adding or removing Fiori Apps or Tcodes, the Master Catalog and corresponding Spaces/Pages definitions must be updated accordingly.

The Master Catalog is then referenced in the Swimlane Catalog, which contains only the Target Mapping based on design information per swimlane from L4s.

Spaces, Pages and Section Design:

- Space definitions will follow L2-level information.
- Page designs will be based on L3-level information.
- Sections within each Page will follow L4-level information.

This structure is aligned with the process models designed by the project team, ensuring a 1:1 match so users can easily identify the relevant processes. L5 represents the process steps in SAP Signavio, which contain the Fiori Apps, and Tcodes for the swim lane.

Role Implementation and Import:

For each role, the relevant Spaces must be added along with the Swimlane Catalog containing Fiori App/Transaction Code information.

Once these roles are built in S/4 HANA, they will be imported into the SAP Build Work Zone as either Single or Composite Roles. The roles will be periodically replicated to sync role information with the SAP Build Work Zone, ensuring that the most recent changes in the Role Menu structure, including Spaces, Pages, and Sections, are reflected.

Database Security

Authentication

Typically, direct access to the underlying database is only required for administrators, some developers, and certain integration processes. If such connectivity is required, the following authentication methods are to be used:

- **Basic Authentication**: Used only for non-interactive access by ETL tools, or other integration processes which must programmatically access the database. Users such as developers or administrators will **not** authenticate using their username and password.
- **SAML**: Interactive access to the database for developers or administrators will use Single Sign-On via the SAML protocol.

User Authorisation and Provisioning

Administrators and developers are given the necessary access to the HANA database, while business users typically do not need direct access. Restricted user accounts are created for business users, where logon is disabled. These users, particularly those accessing SAC Dashboards, are only granted SELECT privileges for relevant calculation views.

Auditing and Monitoring

Auditing provides Syensqo with the ability to monitor user activities performed in the system. An audit policy defines the actions to be monitored and the conditions that make those actions relevant for auditing. When such an action occurs, the policy is triggered, and an audit event is recorded in the audit trail.

Logging and auditing every database transaction will not be feasible for an S/4HANA system which executes tens of thousands of database operations per minute. However critical system administration functions in the SYSTEMDB or similar will be audited using HANA-native features.

Logs are written to SYSLOG at the operating system and can be integrated to SIEM tools. The exact design for this will be determined during detailed design in cooperation with Syensqo's cybersecurity team.

Encryption

The HANA database provides for data files, log files, and backups to be encrypted. In line with the overall security principles, this will be used for all HANA databases.

Not all systems in scope of the ERP Rebuild program will run on HANA. The use of SQLServer is recommended from a security perspective due to the superior encryption capabilities compared to Sybase ASE.

Authorisations in SuccessFactors

SAP SuccessFactors provides a robust framework for managing user access and ensuring the security of sensitive data through various authorization concepts. These concepts are essential for enforcing access controls, complying with regulatory requirements like GDPR, and protecting sensitive data (PII).

Key Authorisation Concepts

Role-Based Permissions (RBP)

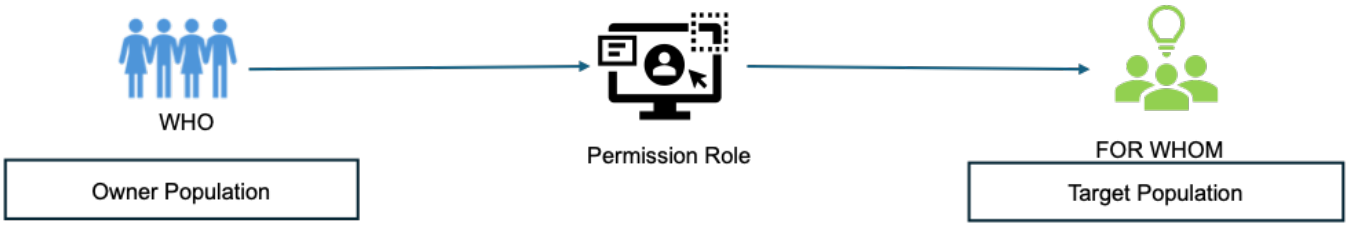
- **Core Authorization Model:** SuccessFactors primarily uses Role-Based Permissions (RBP) to control access to system functions, modules, and data. RBP allows administrators to define permissions based on roles, which are then assigned to users or groups.
- **Granular Control:** With RBP, administrators can grant or restrict access at a granular level, including specific modules (e.g., Employee Central, Performance Management), data fields, and even specific actions (e.g., view, edit, delete).

Permission Groups

- **Grouping Users:** Users are grouped based on attributes like job role, location, or department. These groups are then linked to permission roles, ensuring that access is aligned with organizational structures and responsibilities.

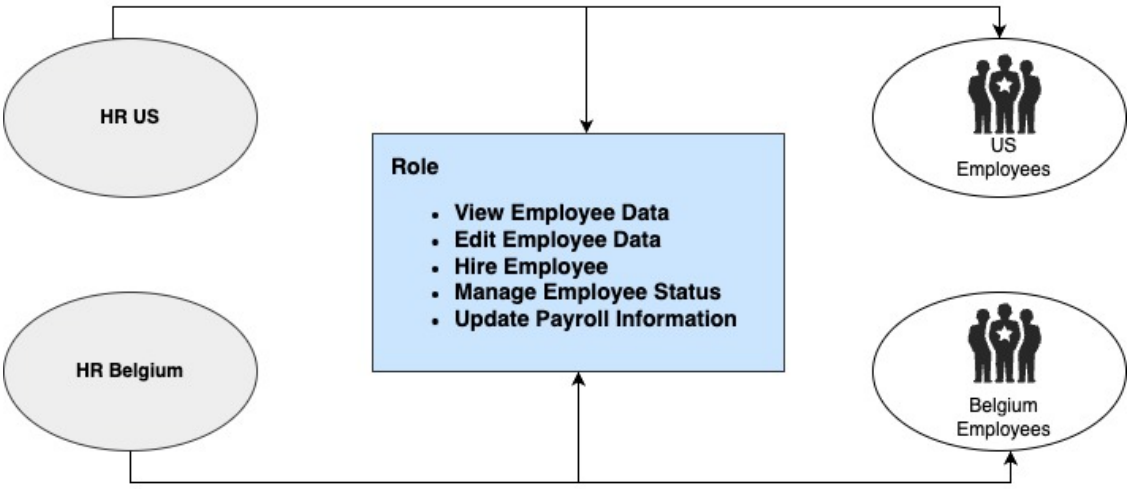
Dynamic Groups

- **Automated Updates:** Dynamic Groups in SuccessFactors automatically update membership based on defined criteria (e.g., job title, hire date), ensuring that access rights remain current as user attributes change.



These groups are segmented into two populations:

- **Owner Population:** The grantor group, which includes users assigned with permission roles.
- **Target Population:** The group of users who can be accessed using the assigned permissions.



A key design recommendation is to create roles based on country, with each country having designated fields and permissions mapped according to business and compliance requirements.

Employee Self Service (ESS) and Manager Self Service (MSS) roles are dynamically assigned to users based on their job and country as indicated in their employee master data. The permissions for ESS and MSS roles are designed to cover all necessary functionalities for employees and managers, respectively.

Additional roles are created as needed for HR administration activities, such as Employee Central, Payroll Managers, Learning Administrators, Onboarding/Offboarding, and Performance Management, and are mapped to the respective job roles.

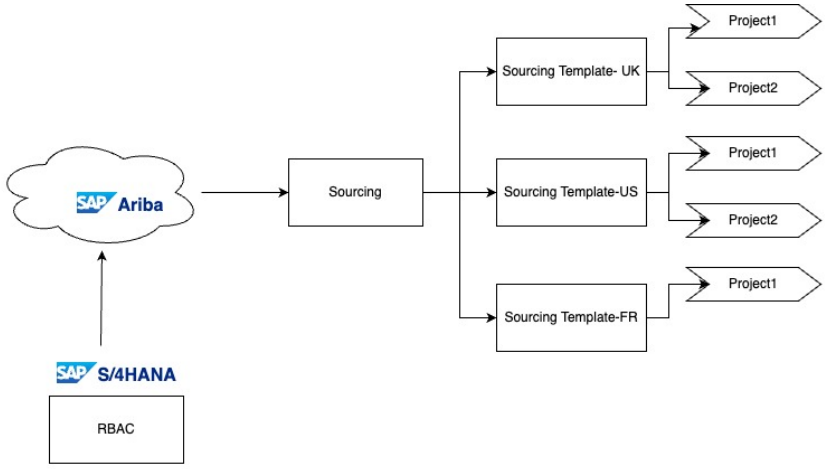
All sensitive data, including PII in SuccessFactors, must be protected and comply with regulatory requirements by adhering to the security principles outlined above.

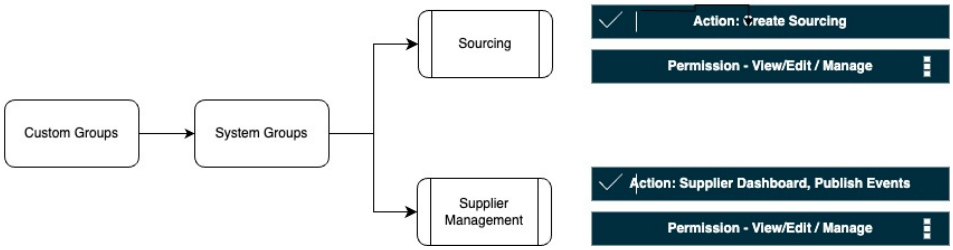
Further details regarding roles and permissions will be defined or revised as part of the SuccessFactors project.

Authorisations in Ariba

SAP Ariba utilizes Role-Based Access Control (RBAC) to manage user access. This means that user permissions are assigned based on their job within the organization. Each group corresponds to a specific set of tasks or responsibilities within the SAP Ariba platform.

- **Standard Groups:** SAP Ariba provides several standard groups that are pre-configured for typical user needs, such as Procurement Manager, Buyer, Supplier, and System Administrator.
- **Custom Groups:** Custom groups are tailored to specific needs, allowing for a more granular level of control over user permissions.





Authorization checks related to procurement activities are performed in S/4 HANA using RBAC and then pushed to Ariba.

In Ariba, users can be restricted based on templates specific to a country. A sourcing template is created with the relevant attributes and fields, and access is assigned only to users from the same country. For example, users from the UK or Belgium will be mapped to their respective country's sourcing template.

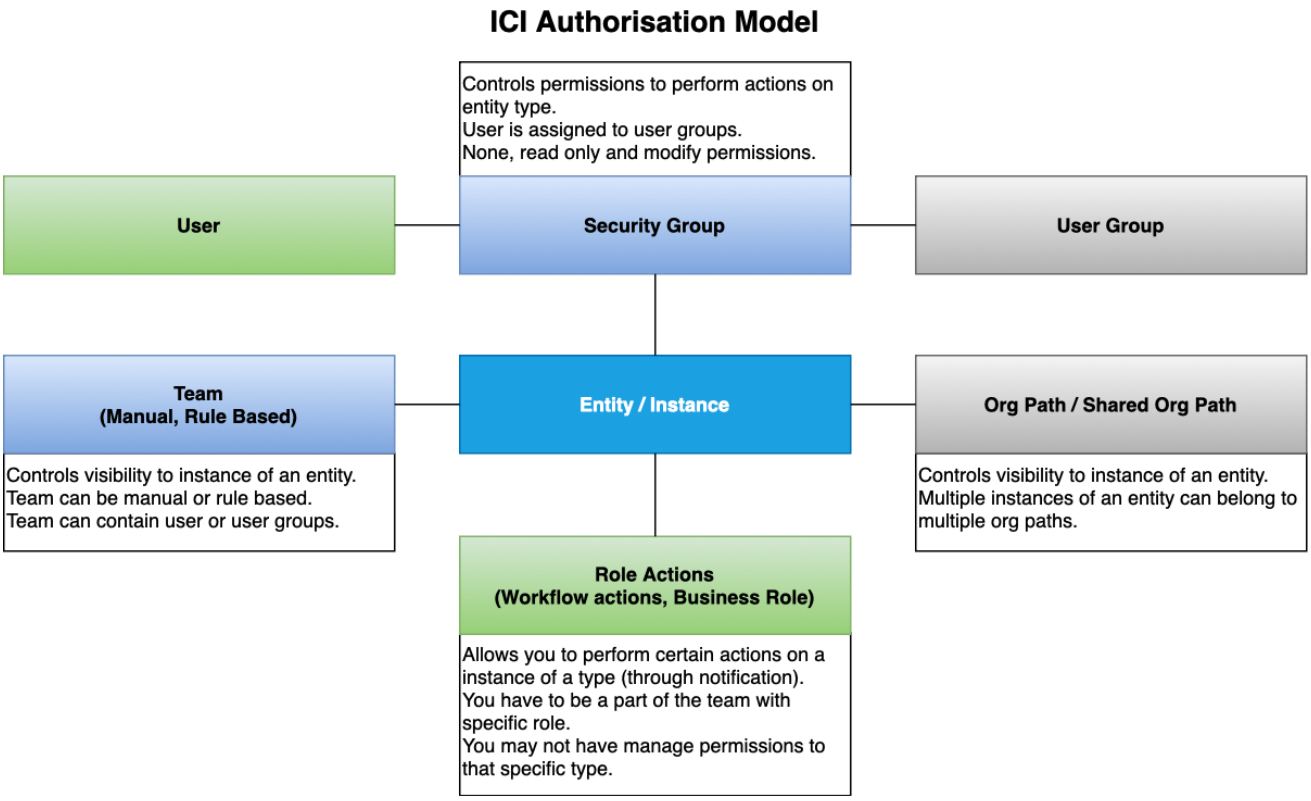
The sourcing template can also be linked to multiple projects, with each project being assigned to a user as the project owner.

For Ariba Buyer/Supplier, the access design follows the same custom groups, tailored to specific business needs. Any additional requirements will be evaluated during the detailed design phase.

Authorisations in ICertis

Standard Single - Tenant deployment with access restrictions using ICI Authorisation Model

ICertis Contract Intelligence (ICI) will be deployed in Single Tenant (ST) Deployment model in a region aligned to the rest of the landscape.



Every Syensqo user will be assigned a position in the organisation at that node of the hierarchy, or at nodes below that node. Syensqo can configure region-specific Org Units.

Authorisations in ICertis will be driven by Org structure, Security Groups configured by Syensqo.

All data and all contract documents will be stored in same deployed region, but users will access it based on their permission assigned. For example, China users will have access to only those contracts which are under “China Org”, However US Legal can have access to contracts for US as well as China.

Authorisations in Reporting Tools

Reporting is conducted through SAC, where live reports are queried from S/4 HANA and DataSphere. Access to S/4 HANA reports is governed by S/4 HANA authorizations. In SAC, access is managed via Teams, which are mapped to specific dashboards. These teams are then linked to jobs in IAG to facilitate provisioning.

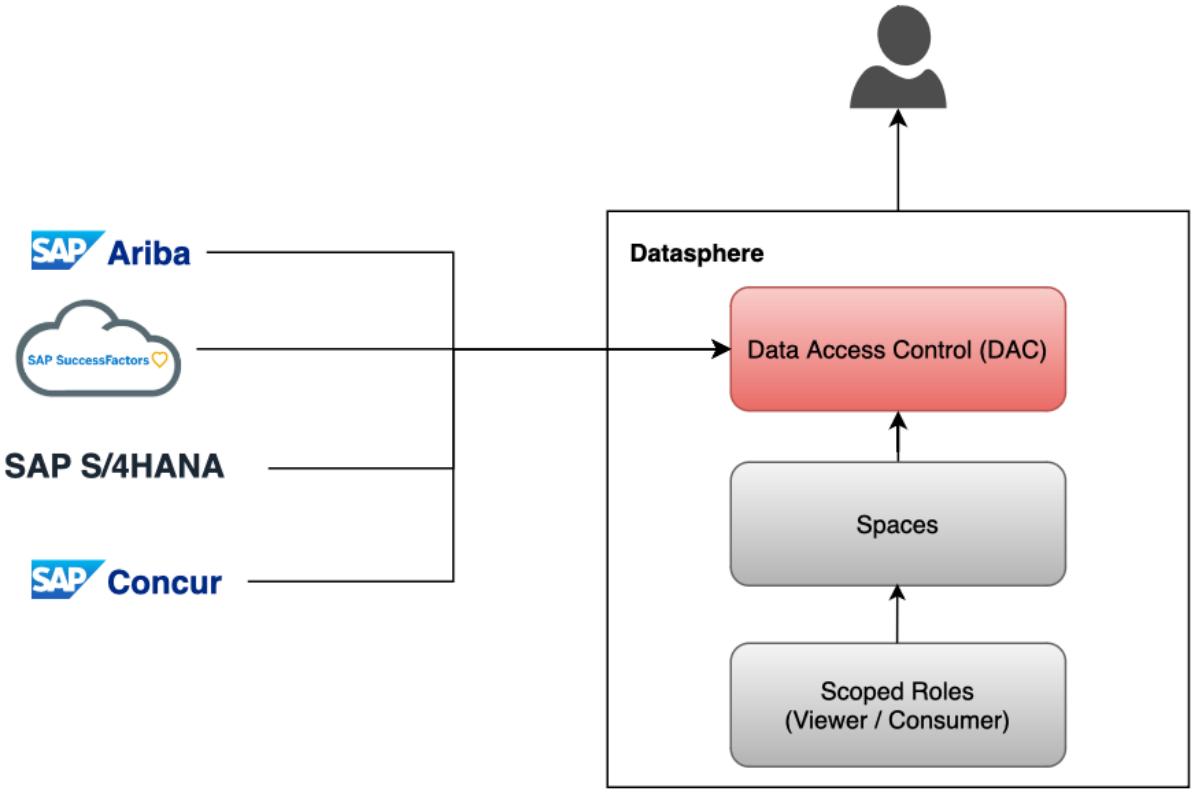
In Datasphere, reporting authorization is designed to mirror the access controls and data restrictions applied within the core S/4 HANA system. This ensures that users have consistent access across both transactional and reporting layers, aligning their permissions with their roles and responsibilities within the organization.

Consistency with S/4 HANA Authorizations

Mirroring Access: The reporting layer in Datasphere is configured to mimic the same access controls as those defined within the core S/4 HANA system. This means that the data a user can view or interact with in reports is consistent with their access rights in the transactional system.

Data Security and Compliance

Controlled Data Access: By mirroring S/4 HANA authorizations in the reporting layer of Datasphere, it can ensure that sensitive data is protected and only accessible to users who are authorized to view it. This alignment helps in maintaining data security and compliance with internal policies and regulatory requirements.



The relevant authorizations are imported from various applications into DataSphere, forming Data Access Controls (DAC). Access is mirrored from S/4 HANA, and most data restrictions in Datasphere are enforced based on S/4 HANA authorizations.

Reports in relevant SaaS applications follow application-specific access, based on users job roles, allowing them to execute reports as needed.

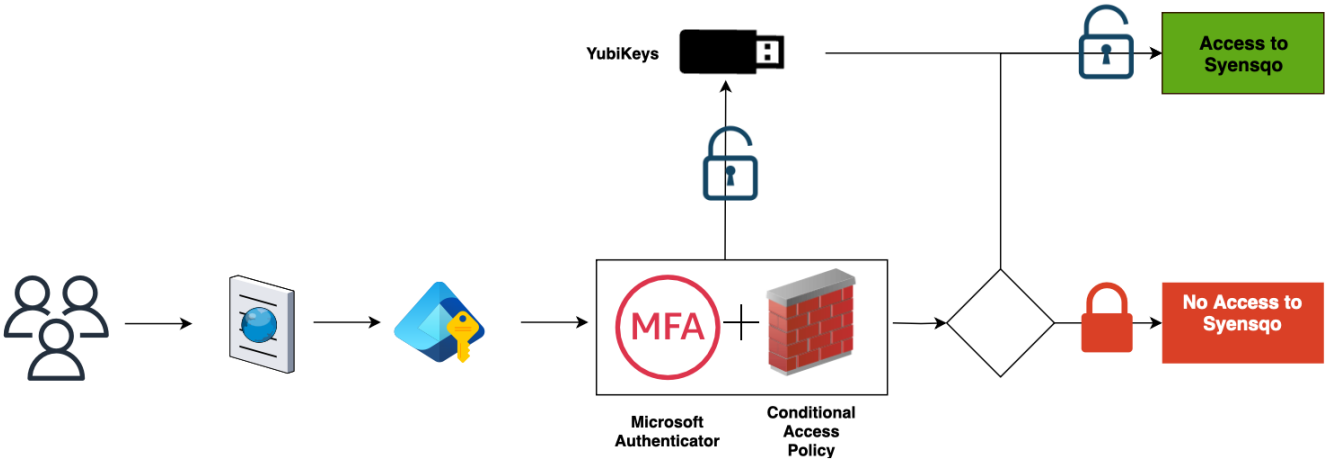
Reporting tools like QlikView, Tableau, and DataOcean are currently out of scope. The teams responsible for these tools must ensure compliance with the Security Principles outlined above.

Authorisations in CRM

The decision between CX and CRM applications is still pending as of the time of writing this document. The application security functionality will be further developed based on the principles outlined above and will be further evaluated during the detailed design phase.

Authentication

Authentication is the process of verifying the identity of a user, device, or system before granting access to a resource, system, or application. It is a critical aspect of security that ensures only authorized individuals or entities can access sensitive information or perform certain actions within an IT environment.



A user logs into Syensqo using their credentials (username and password) to verify their identity, along with mandatory Multi-Factor Authentication (MFA), which enhances security by combining something you know (password) with something you have (phone). Some users utilize YubiKeys for an additional layer of authentication when accessing sensitive systems.

The project recommends to transition from Trustbuilder/InWebo to Microsoft Authenticator for a number of security reasons.

First, Microsoft's use of 'number matching' offers better protection against account take-over via MFA fatigue attacks, in which users are bombarded with constant MFA authorisation push notifications until they click "Accept".

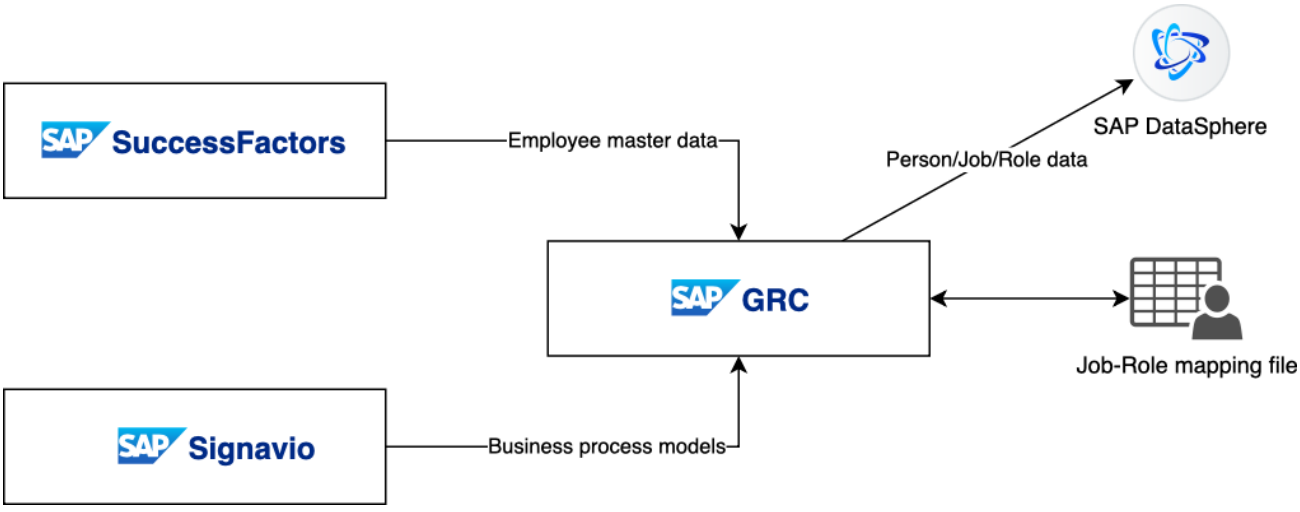
Second, Microsoft Authenticator records the geolocation of both the login terminal and mobile device used to complete the MFA step. These location data can be used in Attribute-based authorisation decisions to permit or deny access to export-controlled data. This can prevent otherwise-authorized users from accessing export-controlled data while they are travelling away from their usual location and are thus accessing the system remotely. Transitioning towards a MFA product suite which geolocates users at the point of authentication, and using their second-factor device rather than only the IP address of their workstation (which might be obscured via VPNs and other mechanisms), will be essential to fully complying with export controls.

Single Sign-On

All access will be via Single Sign-On against Syensqo's corporate Identity Provider. No end user will be issued with passwords or have the ability to set a password. A limited number of "break-glass" accounts may be established to preserve administrative access even during interruptions of the integration with the Identity Provider. These credentials will be protected such that they can only be used by the joint and concurrent action of two individuals (e.g. two trusted administrators will each hold one half of a long and random password").

User-Job-Role Mapping

User-Job-Role Mapping is an important activity in SAP programs, ensuring that users are granted the appropriate level of access needed to perform their job functions efficiently while maintaining security and compliance. This process involves systematically aligning users with specific job roles within the organization and assigning the corresponding SAP roles that determine their permissions within the system.



The process-level information from SAP Signavio is extracted to SAP GRC particularly L4 and L5 details, which include roles, transaction codes, and Fiori apps. This data is then mapped to job definitions from SuccessFactors and roles within the organization.

Job to Role Mapping is a critical component of SAP security and user management. It involves aligning job functions within the organization to specific process roles, ensuring that employees have the correct access rights to perform their duties while maintaining security and compliance. Generally, this activity managed in Excel by Business Leads in collaboration with HR, who facilitate discussions to ensure accurate mappings. Given its importance, this information needs to be systematically documented.

A custom program will be developed to maintain Job-Role mapping by Business Leads. The data is then integrated with the Process Information Report (PIR) to generate a consolidated report in Datasphere. This report will serve as a single source of truth for Security Teams, aiding in role building and managing user access, as well as governance processes related to transaction codes and Fiori apps.

As this report contains critical information about users, jobs, and processes, it will be utilized by Business Leads and the Risk Team in their daily operations.

SAP User Provisioning

User Provisioning is a vital process for managing user access in SAP & non-SAP environments. By following best practices and leveraging automation, organizations can ensure that their users have the necessary access to perform their jobs effectively while maintaining strong security and compliance controls.

? Unknown Attachment

SuccessFactors acts as the single source of truth, with real-time user attributes regularly updated. A job runs every 4 hours between SuccessFactors and IdentityNow, extracting information such as first name, last name, and other required fields (JML Actions) to provision or deprovision users in Entra ID. For new users, Entra ID generates the SAMaccountname and email, which are then fed back into SuccessFactors to update the UserID and email fields in the SF application. For movers and leavers, Entra ID executes the appropriate actions as configured in IdentityNow. This data serves as the basis for provisioning user access across multiple SAP landscapes in Syensqo.

SuccessFactors functions as the source system for Identity Access Governance (IAG), which pulls user-related information using **HR Triggers** and initiates actions based on configured rules.

IAG is a cloud-based platform offering services such as **Access Risk Analysis**, **Access Request Management**, **Business Role Design** and **Access Certification**. It includes a feature called **'Job Business Roles**,' where roles from various enterprise systems are stored according to mappings provided by Business Leads, ensuring they are maintained and up-to-date. IAG uses connectors to provision access to multiple cloud and on-premise systems through cloud connectors, enabling comprehensive enterprise provisioning.

Based on **JML** (Joiners, Movers, Leavers) actions, IAG assigns the appropriate 'Job Business Role' to users based on their Job ID and completes provisioning in the target systems. During provisioning, IAG performs real-time Segregation of Duties (SoD) checks to detect any conflicts with the assigned role. If any SoD violations are found, a workflow notification is triggered to the Line Manager and Role Owner for analysis, review, and either rejection or mitigation. If no SoD violations are detected, no workflow is triggered, and provisioning to the target systems proceeds according to the Job Business Role definition across enterprise systems.

The GRC On-Premise application is essential because IAG has limitations in its PAM functionality, which only supports S/4 HANA and not web-based applications like Fiori. Therefore, it is recommended to use the GRC On-Premise application to effectively utilize the EAM functionality in GRC AC, allowing the use of Role-Based ID functionality where FF roles are directly assigned to users in the target system to support Fiori apps or other web-based applications.

Additionally, since IAG does not support Process Controls functionality, the GRC On-Premise application is necessary to document robust controls and mitigate risks as needed using GRC Process Controls.

Provisioning Flow

? Unknown Attachment

SAP Cloud Identity Access Governance (IAG) solution includes HR Trigger functionality that allows automatic creation of access requests based on JML Actions and the rules configured in HR Triggers. The IAG is integrated with SAP SuccessFactors Employee Central, enabling the capture of changes to employment status in the HR system and the automatic initiation of access requests through IAG. These requests follow a defined workflow and are provisioned to target applications (both cloud and on-premise) using predefined job business roles.

During the provisioning process to target systems (both cloud and on-premise), IAG performs checks for any Segregation of Duties (SoD) violations, including both system-specific and cross-system conflicts. If violations are detected, a workflow is triggered for the relevant Role Owner or Risk Owner to review, analyse, reject, or mitigate the conflicts, enabling the provisioning to proceed. This workflow is initiated only in the presence of SoD violations; otherwise, the provisioning process continues uninterrupted and completes the user provisioning in the connected target systems.

SAP IAG Connection Channels

Application	Channel	Standard Connector	Custom Connector

S/4 HANA	Cloud Connector	Yes	No
GTS	Cloud Connector	Yes	No
GRC	Cloud Connector	Yes	No
SuccessFactors	IPS	Yes	No
Ariba	IPS	Yes	No
SAC	IPS	Yes	No
Datasphere	IPS	Yes	No

SAP GRC Access Controls

Segregation of Duties

Segregation of Duties (SoD) is a critical concept in GRC Access Control that focuses on minimizing the risk of fraud and errors by ensuring that no single individual has control over all aspects of any critical business process. By separating responsibilities among different individuals or roles, organizations can reduce the potential for conflicts of interest and unauthorized activities.

SoD Ruleset Design Overview

The ruleset is a global container for all generated rules in IAG which is being utilised to report access risks on the role, profile and user level.

- SAP IAG comes with a delivered S4H & SaaS standard ruleset that can be leveraged for Syensqo.
- Standard delivered ruleset to be adopted and reviewed to deliver rules that best fit Syensqo.
- Custom Developments undertaken during various stages of the project will also be considered and if necessary, included in the AC ruleset for GRC Ruleset inclusion. These will be mapped to the closest relevant standard function within the GRC IAG Ruleset.

Risk comprises of function/s which violates company policies resulting to fraud, data manipulation, and system failure or asset losses. Risk is also categorised by criticality rating of High, Medium or Low.

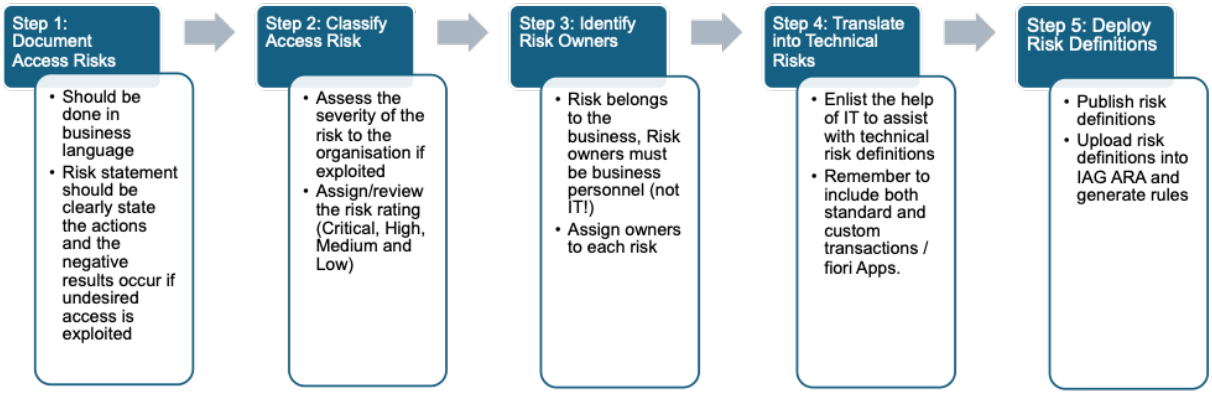
There are two types of risks as follows:

- **SoD Risks:** Type of risk consisting of two or more conflicting function. This type of risk occurs when a user can execute multiple processes which would present opportunity for fraud, loss or other damage.
- **Critical Risk:** Type of risk which contains only one function. User will have risk once assigned to a transaction belonging to a critical function.

Functions are a grouping of one or more related actions and/or permissions for a specific business area.

Access Controls Ruleset Approach

According to best practices, the following steps should be followed when developing the ruleset for Syensqo. The SAP-standard AC risk ruleset will serve as the baseline. Custom risks may be added to the ruleset based on input from the responsible Business Leads. However, SAP-delivered rules will not be modified or removed; they can only be activated or deactivated within the ruleset.



Mitigating Controls

GRC SoD Mitigating Controls lies in their ability to safeguard against risks associated with role conflicts and to ensure compliance with regulatory requirements. Leveraging these controls from GRC Process Controls enhances their effectiveness by providing a structured, automated, and integrated approach to managing and mitigating risks across the organization. This approach not only strengthens the organization's risk management framework but also ensures the integrity and reliability of its business processes.

Segregation of Duties Analysis at System Level

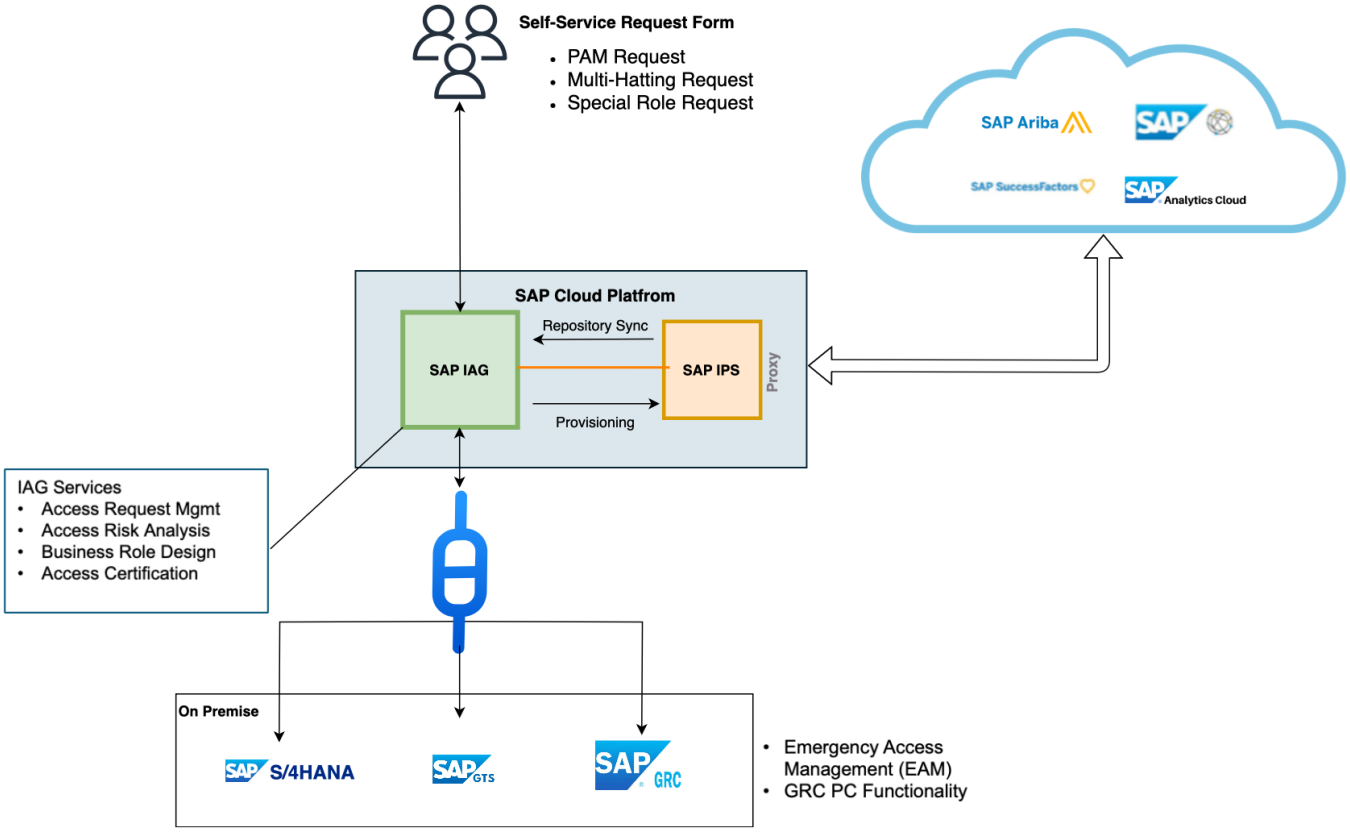
SoD analysis is conducted during the Role Design and Build phases to ensure that roles across different L4 processes are free from SoD conflicts. If conflicts are identified, the conflicting Tcodes / Fiori Apps are either removed or moved to another role to create a SoD-free role. This practice ensures that process roles remain clean and compliant, making the role mapping exercise smoother by reducing conflicts at the Composite Role level and simplifying the remediation process for adding or removing roles.

SoD checks are performed primarily at the Master Role, Composite Role, and User levels, with the goal of keeping roles SoD-free through remediation or by mitigating risks with robust controls.

Cross-System Analysis

Cross-System Segregation of Duties (SoD) analysis is a critical analysis in ensuring the security and compliance of integrated enterprise systems. When SAP S/4HANA uses in conjunction with other SaaS applications like SuccessFactors, Ariba, and others the complexity of managing SoD risks increases significantly. This is because users often have access to multiple systems, and the potential for conflicting duties that could lead to fraud or compliance violations spans across these platforms.

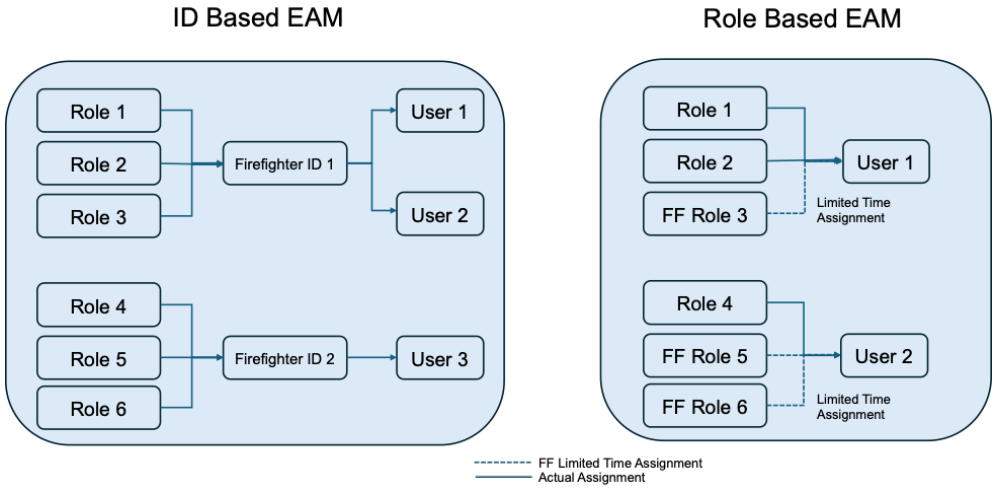
This is basically achieved using the tool SAP IAG.



Emergency Access Management

Emergency Access Management (EAM) is a critical component within the Governance, Risk, and Compliance (GRC) framework, designed to provide controlled and monitored access to critical systems and data during emergency situations. EAM is essential for managing temporary elevated access rights, ensuring that such access is granted, used, and monitored in a secure and compliant manner.

There are two application types available for EAM: ID-based and Role-based. Only one type can be configured for use at a time.



ID-based EAM Application: A Firefighter ID is a service-type user with elevated privileges in a target system. Administrators create the Firefighter ID in the target system and assign a specific role to it, distinguishing it from other service users. SAP Access Control recognizes this service user as a Firefighter ID by the assignment of the specific role.

The Firefighter ID can be assigned to a user either manually or through an access request. Firefighters can access their assigned Firefighter IDs to conduct a firefight session within validity dates in two ways:

- In the SAP Access Control system using the ABAP GUI and transaction GRAC_EAM (Centralized Firefighting).
- In the target back-end system using the ABAP GUI and transaction /GRCPI/GRIA_EAM (Decentralized Firefighting).

In both scenarios, a new ABAP GUI session opens under the Firefighter ID user, allowing the user to perform emergency activities. A single firefighter can be assigned to multiple Firefighter IDs, and multiple Firefighter IDs can be assigned to a single firefighter. However, only one firefighter can use a Firefighter ID at a time. If a Firefighter ID is in use, a red indicator appears. All changes made during a firefight session are recorded in the change history under the Firefighter ID user, and firefighting logs document the actions with the Firefighter ID, not the firefighter's own user ID.

Role-based EAM Application: Firefighter roles are roles in a target system with elevated privileges, assigned to the user within the SAP Access Control system. The user can access these roles within the specified validity dates. A firefighter logs in to the target system as usual using their own user ID and performs tasks allowed by both their user role and the assigned Firefighter role. When the user engages in a transaction included in the Firefighter role, it initiates a firefight session. Transactions and changes are logged with the firefighter's own user ID.

In both ID-based and Role-based EAM scenarios, administrators manage the assignment of firefighter owners and controllers for Firefighter IDs/roles in the SAP Access Control system. Typically, firefighters request access to Firefighter IDs/roles for specific validity dates through an access request, followed by an approval process. Administrators can also assign Firefighter IDs/roles to firefighters without requiring approval.

Due to the limitations of GRC EAM with web-based applications and Fiori apps, we will adopt the **Role-Based EAM approach**. This approach enables assigning the required Firefighter roles to the user for a limited period, enabling them to perform firefighter activities using their own ID across both GUI and Fiori apps.

EAM for SaaS Applications

Since SaaS applications do not provide logs similar to GRC EAM for S/4 HANA, where detailed activities are recorded when a user logs in using Firefighter, there is a need to explore third-party tools that can efficiently log user activity in SaaS applications. This will be further evaluated during the detailed design phase.

Access Request Management

Access Request Management (ARM) is a key component of the SAP IAG. ARM streamlines and automates the process of managing user access requests, ensuring that the right users have the right access at the right time.

Using ARM functionality, the self-request form is configured to allow requests for multi-hatting, privileged access management that falls outside of your regular 'Job Business Role'. This form follows a standard template, routing the request to the Line Manager, Role Owner, and Risk Owner for in-principle approval before assigning the roles to users. This process includes Segregation of Duties (SoD) conflict checks to ensure compliant access is provisioned to the users.

User Access Reviews

SAP IAG provides a robust framework for managing user access and ensuring compliance with regulatory requirements. One of its key features is the User Access Review functionality now being called as Access Certifications, which helps organizations maintain appropriate access levels and prevent unauthorized access to sensitive data.

User Access Reviews for roles assigned based on jobs in SuccessFactors do not require additional review, as these roles are continuously evaluated by the respective Business Leads through the Job-Role mapping process to ensure the necessary access aligns with job responsibilities.

However, access granted for multi-hatting roles or IT support roles must be reviewed every six months to validate whether the need for such access still exists. It is recommended to conduct periodic access reviews for multi-hatting and IT support roles as outlined below.

Process for Multi-Hatting and Support Roles Review:

- Must be reviewed every 6 months
- A Job is scheduled biannually, during which the respective Business Leads must review and confirm whether the user's access remains appropriate.

Summary of Decisions Deferred to Detailed Design

The following topics have been deferred to the Detailed Design stage as their resolution cannot be performed with the limited time available during Conceptual Design. The outcomes of these decisions are important for the solution overall, but have relatively little impact on the delivery cost and effort estimates which are one primary deliverable of the Conceptual Design phase during which this document was written.

- SuccessFactors RBP Design will be documented in the SF Optimisation Project
- CX/CRM Application Decision to be followed
- Replacement, or improvement and integration of, Access Flag Tool.
- Icertis and Keelvar Applications for Ariba
- Emergency Access Management for SaaS Applications
- Role design for the applications in scope
- SoD rules for each application
- Auditing and monitoring the logs with cybersecurity