

ISVG AND SAP – A TECHNICAL OVERVIEW

This paper is a technical exploration of the integrations between IBM Security Verify Governance (ISVG) and SAP. The focus is on the native ISVG SAP Connector not the IM SAP Provisioning Adapters that can work with the ISVG Broker.

The paper presents an overview of the components and flow, and then explores the various integration points and functions.

Many thanks to the ISVG technical people who have helped with content for this paper, in particular:

- Fabrino Calvarese – Development Manager – Identity Governance
- Fabrizio Tarallo – Software Engineer – Identity Governance
- Diego Fiorani – Software Engineer – Identity Governance
- Alberto Novello – Security Lab Services – Identity Governance
- Marco Venuti – WW Tech Sales Leader – Identity Governance

For any comments/corrections, please contact Amit Chaudhary (amit.chaudhary@in.ibm.com).

Contents

Overview of ISVG and SAP Integration	4
Identities and the SAP Connector “HR Feed”	6
Identities in SAP HR	6
SAP Connector “HR Feed” Configuration	7
ISVG and SAP Governance and Provisioning	9
Intro to SAP Security	9
SAP Users (Accounts)	9
SAP Transactions and other Authorization Objects	11
SAP Roles	13
Coarse-Grained (Enterprise) Governance	14
SAP Objects Loaded	14
Enterprise SoD	16
Fine-Grained (SAP-Specific) Governance	19
SAP Authorization Objects in ISVG	19
ISVG SAP Authorization Patterns (or Risk Entitlements)	20
Defining SAP Risk in ARCS	25
SAP Role Violations	27
SAP Authorization Violations	27
User Violations	28
How Well are the Roles Named?	29
Role Warnings (Bad Practice Analysis for SAP Access Control Model)	30
SAP-specific Reporting in ISVG	30
Where Does All the Data Come from?	32
Loading Identities into ISVG	33
Loading SAP Accounts and Permissions	33
Loading SAP Fine-grained Authorization Objects	33
Loading SAP Authorization Patterns	33
Loading Business Activities	34
Loading Business Activity to SAP Authorization Pattern Mapping	34
Loading Risk Definitions	34
Technical Aspects of the SAP Connectors and Tasks	34
ISVG SAP Connector (for AGC and ARC)	35
ISVG SAP Connector Agent (for ARCS)	37
Synchronising Fine-Grained (ARCS) to Coarse-Grained (ARC)	39
ARCS Data Refresh Tasks	40
Provisioning with the ISVG SAP Connector	41
SAP Provisioning Adapters	41
SAP HANA Database Provisioning Adapter	41

- SAP NetWeaver42
- SAP Sybase DB.....43
- SAP UME (Portal).....43
- ISVG and the SAP GRC Access Control for SoD Checking.....45
 - Using SAP GRC AC for External SoD Checks46
 - Overview of the Integration.....46
 - Sample Flow with External SoD Check.....46
 - Violation Visibility in ISVG47
 - Task Transfer – SAP GRC AC as a Step in Workflow48
 - Overview of the Integration.....48
 - Sample Flow with Task Transfer49
 - Implications of the Task Transfer Approach50
- Combining the Integrations50

Overview of ISVG and SAP Integration

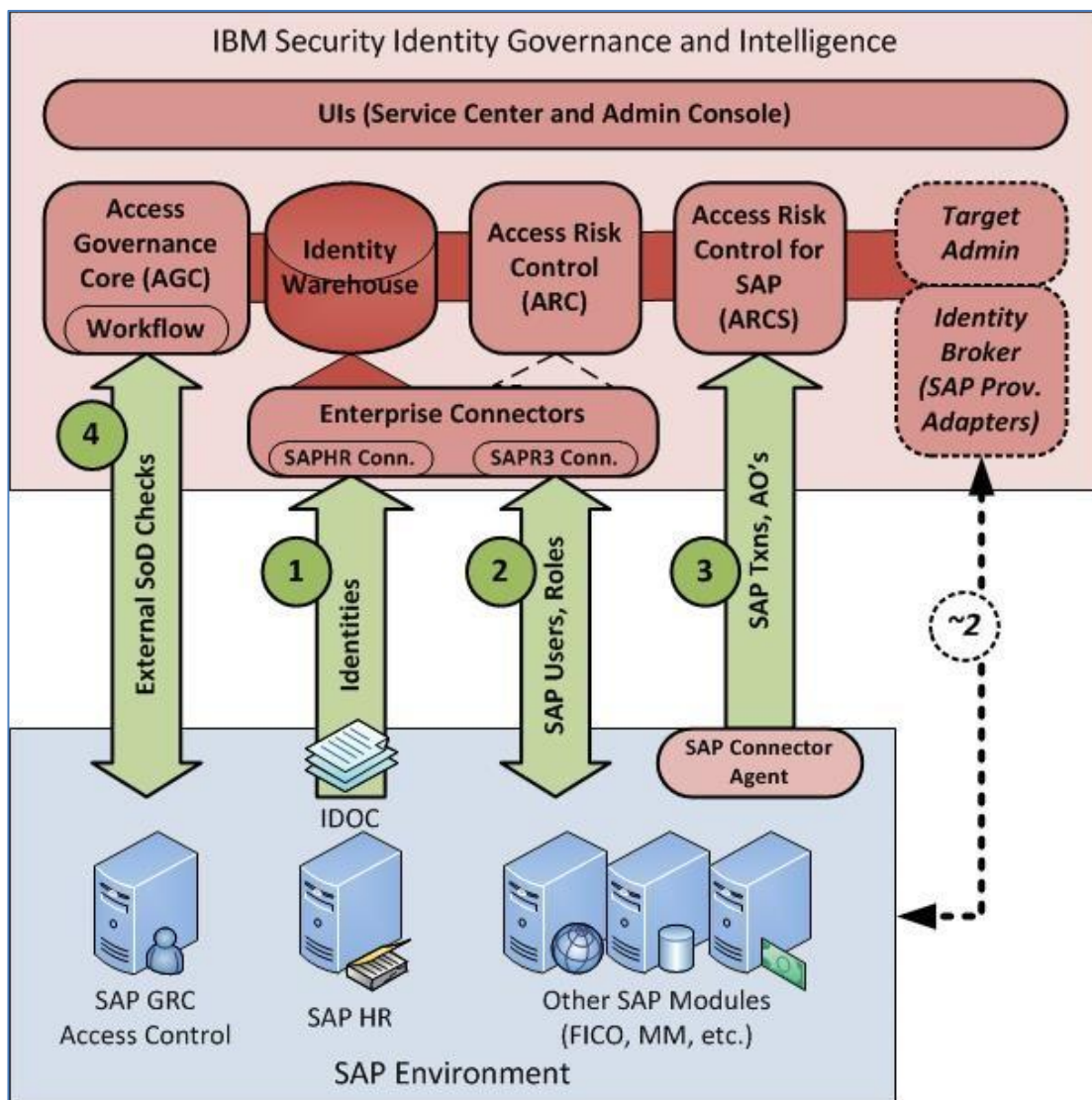
IBM Security Verify Governance (ISVG) provides a number of identity-related functions working with a SAP environment.

Identities are at the center of identity management and governance, and many organizations use SAP as their HR system for employees, contractors and other people. A key integration for ISVG is to consume identities and attributes from SAP HR and use this information to drive provisioning.

Many SAP environments are large and complex, and the access control model supporting it is often large and complex. ISVG provides visibility and governance to both coarse-grained (accounts and roles) and fine-grained (roles, transactions and authorization objects) entitlement in SAP, and can provision accounts and role memberships.

Finally, many organizations already have Separation of Duties policy implemented in SAP GRC Access Control. ISVG can leverage this for its risk decisions.

The following figure summarizes the key components and integration points.



The four integration points are:

1. The SAP Connector can consume identity information from the SAP HR system
2. The SAP Connector can collect SAP User and Role information from SAP for use in enterprise-wide governance, and provision SAP User and Role membership changes back to SAP.
3. The SAP Connector Agent (deployed into the SAP environment) can collect the fine-grained SAP authorization objects, including transactions.
4. ISVG can leverage an existing SAP GRC Access Control installation as an external SoD engine.

Each of these integrations will be explored in detail in later sections of this document.

ISVG uses a data warehouse to hold all objects and this warehouse is leveraged by the various ISVG modules. So, whilst all identities (people in SAP HR), accounts (SAP Users), permissions (SAP Roles) and fine-grained entitlements (SAP Transactions and other SAP AOs) are held in the warehouse, the Core (AGC) and ARC modules present identities, accounts and permissions, and the ARCS module presents the fine-grained entitlements. This is discussed in later sections of the document.

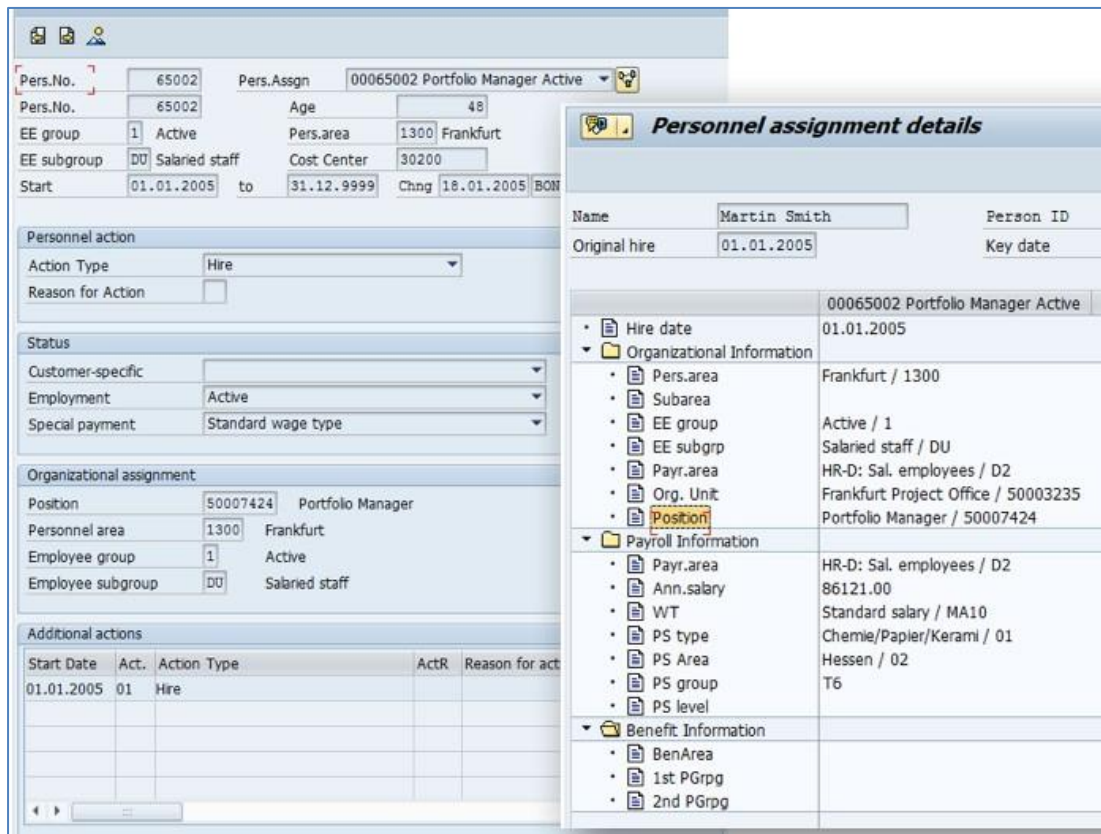
Note that there are also currently four SAP-related (ISIM) Provisioning Adapters that are supported with ISVG via the Identity Broker in the ISVG Virtual Appliance: SAP HANA Database, SAP NetWeaver, SAP Sybase DB, and SAP UME (Portal). From an ISVG perspective they provide the same functions as the ISVG SAP Connector in coarse-grained mode (i.e., reconciliation and provisioning of accounts and permissions). We discuss these modules briefly at the end of the section looking at governance and provisioning.

Identities and the SAP Connector “HR Feed”

This section looks at identities in SAP HR and how the ISVG SAP Connector can act as a HR Feed mechanism. The ISVG SAP (Enterprise) Connector is the only HR Feed mechanism currently shipped with ISVG.

Identities in SAP HR

Identities in SAP HR are Personnel Records. They are represented in a complex set of tables managed by HR. The following figure shows some of the SAP Personnel information for Martin Smith.



The screenshot displays the SAP HR Personnel Record for Martin Smith. The main form shows personal and organizational data, while a detailed view on the right lists specific assignment details.

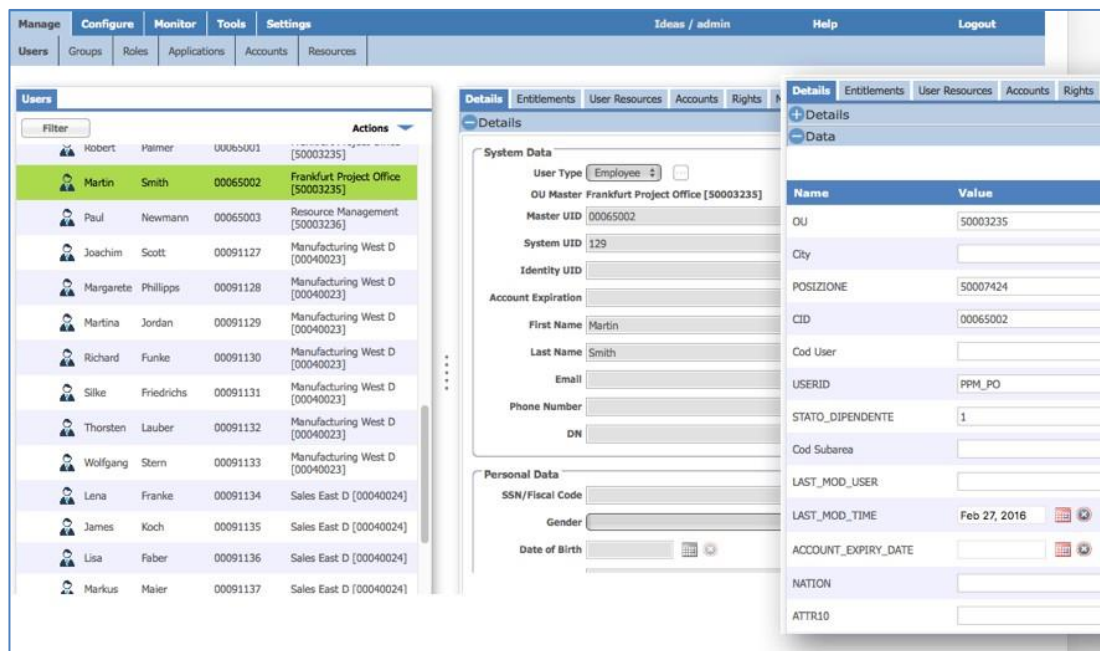
Personal Data	
Pers.No.	65002
Pers.No.	65002
Age	48
EE group	1 Active
EE subgroup	DD Salaried staff
Start	01.01.2005 to 31.12.9999
Chng	18.01.2005 BOM

Personnel assignment details	
Name	Martin Smith
Person ID	
Original hire	01.01.2005
Key date	
	00065002 Portfolio Manager Active
Hire date	01.01.2005
Organizational Information	
Pers.area	Frankfurt / 1300
Subarea	
EE group	Active / 1
EE subgrp	Salaried staff / DU
Payr.area	HR-D: Sal. employees / D2
Org. Unit	Frankfurt Project Office / 50003235
Position	Portfolio Manager / 50007424
Payroll Information	
Payr.area	HR-D: Sal. employees / D2
Ann.salary	86121.00
WT	Standard salary / MA10
PS type	Chemie/Papier/Kerami / 01
PS Area	Hessen / 02
PS group	T6
PS level	
Benefit Information	
BenArea	
1st PGrpg	
2nd PGrpg	

The SAP Personnel Record includes assignment to various other objects. For example, we can see Martin as assigned to the Position of “Portfolio Manager / 50007424” and is in the “Frankfurt Project Office / 50003235” Org Unit.

The SAP Connector will handle the complexity of the multiple connected pieces of information and present it to ISVG.

The SAP Connector will consume all Personnel records and create Identities (Users) in ISVG. The following figure shows Martin Smith from SAP HR in ISVG.

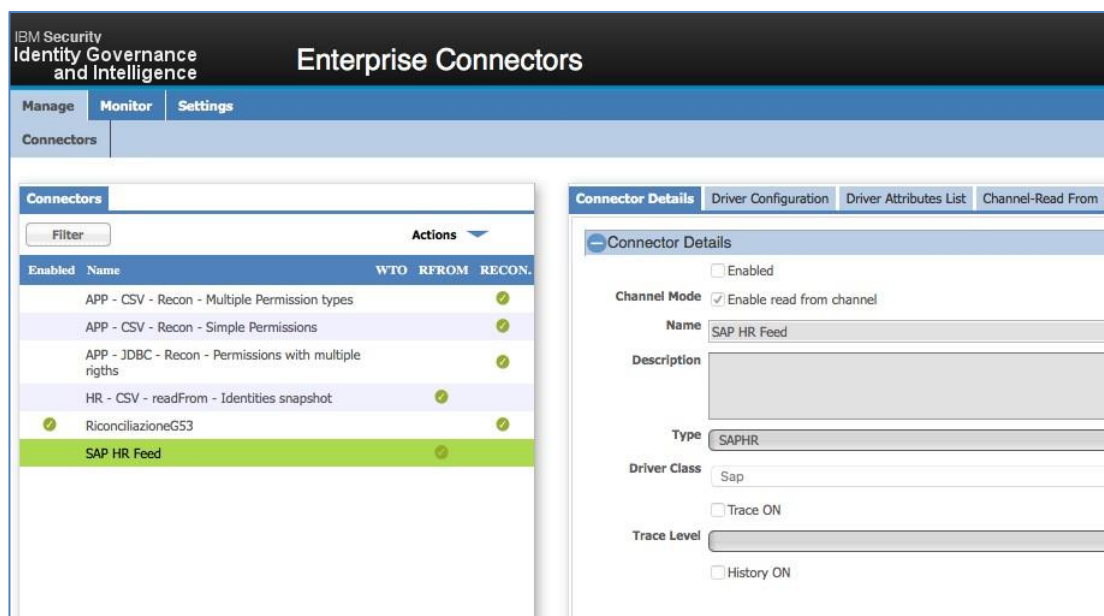


The assignments in SAP HR have been translated into User attributes. The Org Unit in SAP has been used to define the Org Unit in ISVG that the user would belong to.

If there are assignments and these are tied to Attribute Groups in ISVG, then when the attribute group rebuild task is run, changes to the attribute group hierarchies will also be applied.

SAP Connector “HR Feed” Configuration

The SAP Connector for HR Feed is an ISVG Enterprise Connector in ReadFrom (RFROM) mode. An example is shown below.

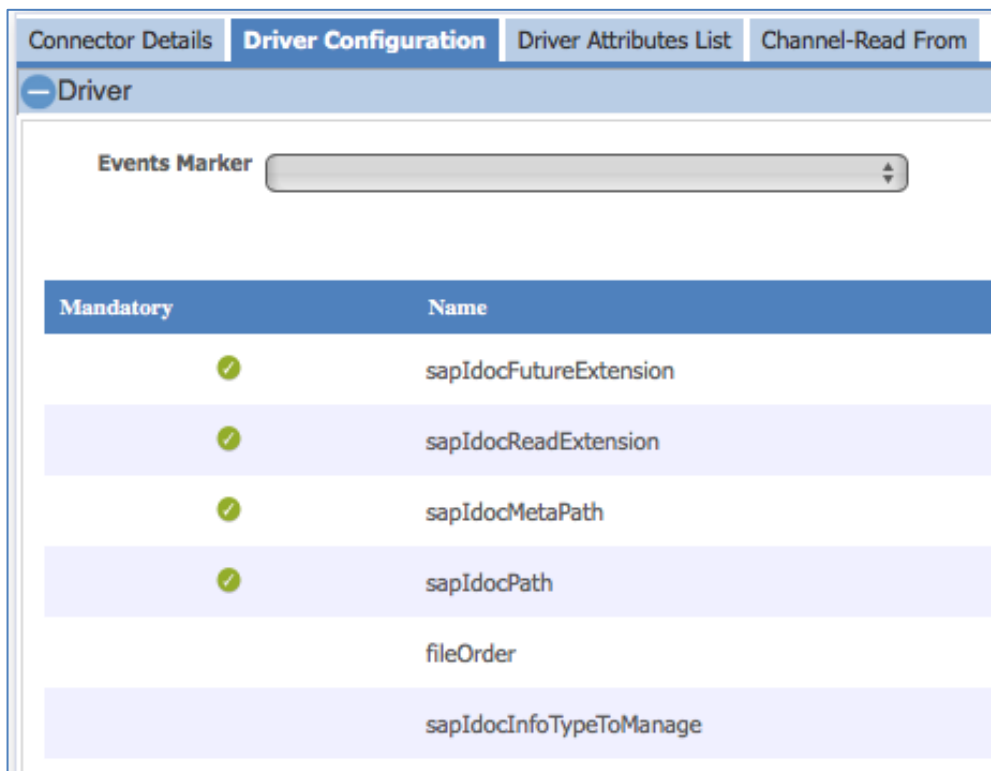


When creating the connector, the key setting is Type. There are two SAP options – SAPR3 and SAPHR. Selecting SAP HR defines is as a HR mode connector. The only driver class available is “Sap.”

The other connector details are the same as for any other Enterprise Connector.

The SAP Connector, when in SAPHR mode, consumes an IDOC file that has been produced by the SAP HR system. It does not connect directly to SAP to pull data.

There are four settings that must be defined for the connector driver and two that are optional.



Mandatory	Name
✓	sapIdocFutureExtension
✓	sapIdocReadExtension
✓	sapIdocMetaPath
✓	sapIdocPath
	fileOrder
	sapIdocInfoTypeToManage

Setting	Description
sapIdocMetaPath	Location where SAP Metadata definition file resides
sapIdocPath	Directory where SAP HR Idoc files are placed

The Connector supports configuring the attribute mapping between the SAP HR system and the ISVG User objects. This is the same as the attribute mapping available with the SAP Connectors when used for reconciliation and provisioning of accounts.

Note that the connector will pull organizational structure (OU) records from SAP HR as well as people (Personnel) records.

ISVG and SAP Governance and Provisioning

This section looks at the governance and provisioning features in ISVG. As the SAP Security model is complex, we provide an introduction to SAP Security before looking at how ISVG can treat SAP security objects in an enterprise-wide context and also the fine-grained SAP-specific features. The section also discusses provisioning with the SAP Connector.

Intro to SAP Security

The SAP Security model is complex and there have been many books written about it. This section provides a brief overview to the depth needed for the ISVG-specific functions.

For users to be able to perform operations in SAP, the user in SAP must have a username, password and a set of authorizations.

The authorization check in SAP has three levels:

1. User and Password: a unique user id and a valid password must be entered in the SAP GUI start screen,
2. Transaction start: every new action is started using a transaction code. The user must be authorized to start a specific transaction.
3. Once the transaction is started, many other authority checks are performed; data (for example a company code) and action (for example view, modify, create).

The latter two are the authorizations.

The following sections provide a simplified view of the key SAP Security objects that will be used in ISVG. It is not complete and may be over simplifying matters from a SAP perspective.

SAP Users (Accounts)

User accounts in SAP are similar to accounts in other systems. They have attributes and operations that can be performed against them (create, change, display, delete, copy, lock/unlock, change password).

Maintain User

User: TUSER-016
Last Changed On: TUSER-016 22.03.2016 07:40:01 Status: Saved

Address Logon data Defaults Parameters Roles Profiles Groups P

Person

Title: Mr.
Last name: Edwards
First name: David
Academic Title: Dr.
Format: Dr. David Edwards
Function:
Department:
Room Number: Floor: Building:

Communication

Language: English
Telephone: Extension:
Mobile Phone:
Fax: Extension:
E-Mail:
Comm. Meth: Remote Mail

Maintain User

User: TUSER-016
Last Changed On: TUSER-016 22.03.2016 07:40:01 Status: Saved

Address Logon data Defaults Parameters Roles Profiles Groups P

Alias: DEDWARDS

User Type: Dialog

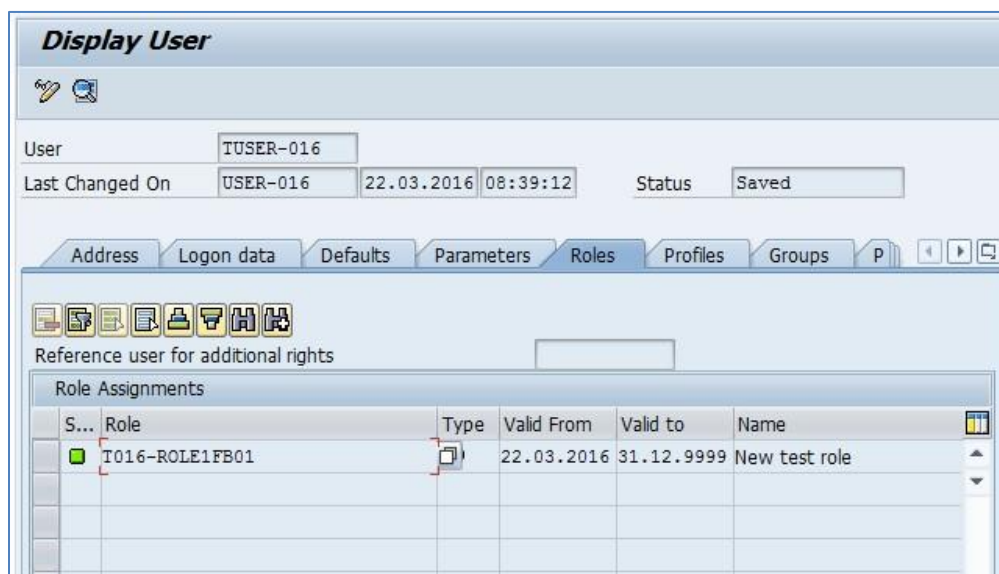
Password

System Differentiates Between Upper- and Lower-Case
Initial password: *****
Repeat password: *****

User Group for Authorization Check

User group: APA Asia Pacific

Users are connected to Roles to provide authorizations.



For example, David Edwards (User TUSER-016) is mapped to the Role T016-ROLE1FB01.

Users are also mapped to Profiles (which are directly tied to Roles) and Groups (used for bulk administration of users).

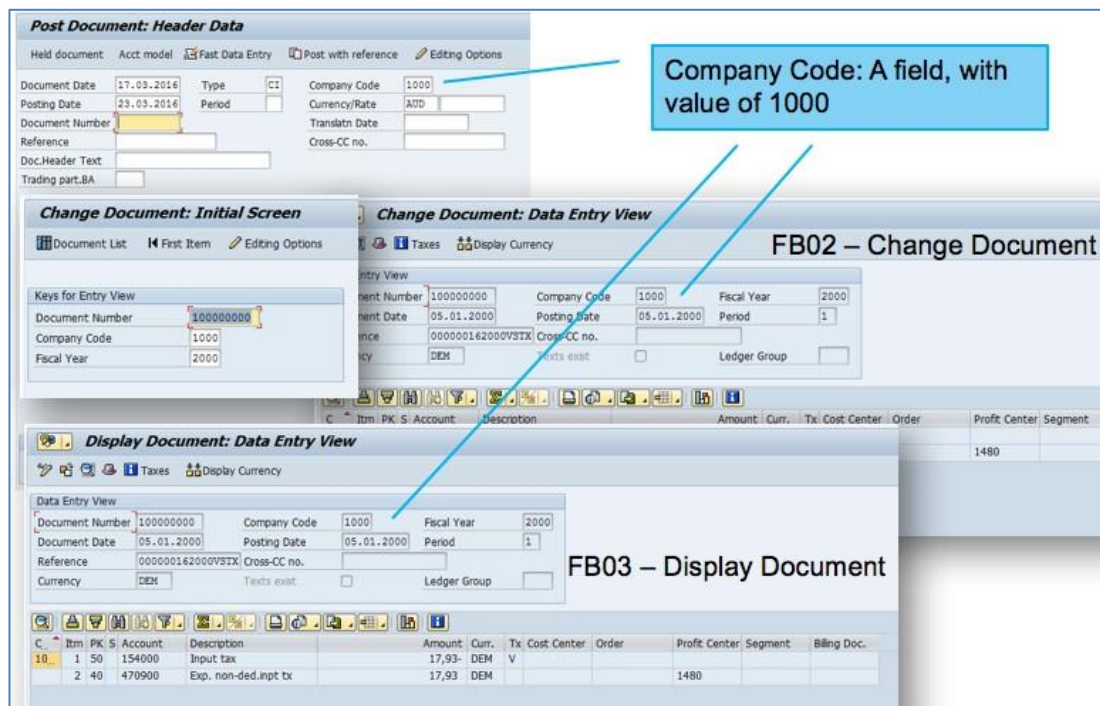
SAP Transactions and other Authorization Objects

A **SAP Role** is a collection of authorizations. It consists of authorization objects. These authorization objects may be transactions, data values or operations.

Transaction, or TCODE, is one type of authorization object. A transaction is a function; a page or set of pages in a SAP module. For example, FB01 is a Post Document (i.e., add financial document), FB02 is Change Document, and FB03 is Display Document. So, all three are SAP Financial transactions that relate to financial documents, each performing a different function (e.g., Add, Modify and View).

Standard transactions are shipped with the different SAP modules. For example, FB01, FB02, and FB03 all belong to SAP Financials (aka FI or FICO). SAP environments may have custom transactions. These tend to start with a "z."

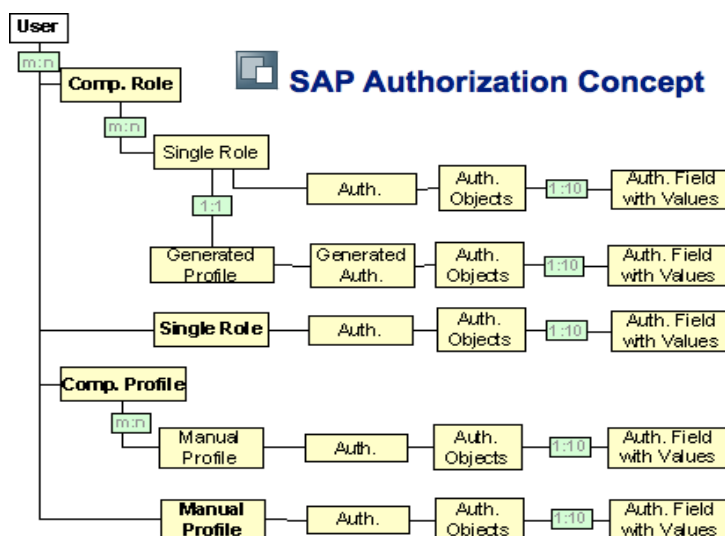
Other **authorization objects** define the data and actions that can be performed on the transaction(s). For example, "company code (BUKRS)" is used to define one or more companies that the SAP installation is for. An authorization object can restrict the data by company code. This value may apply across all similar transactions. The following figure shows the company code across the three FB01/02/03 transactions.



Other data values, like Business Area (GSBER), behave similarly.

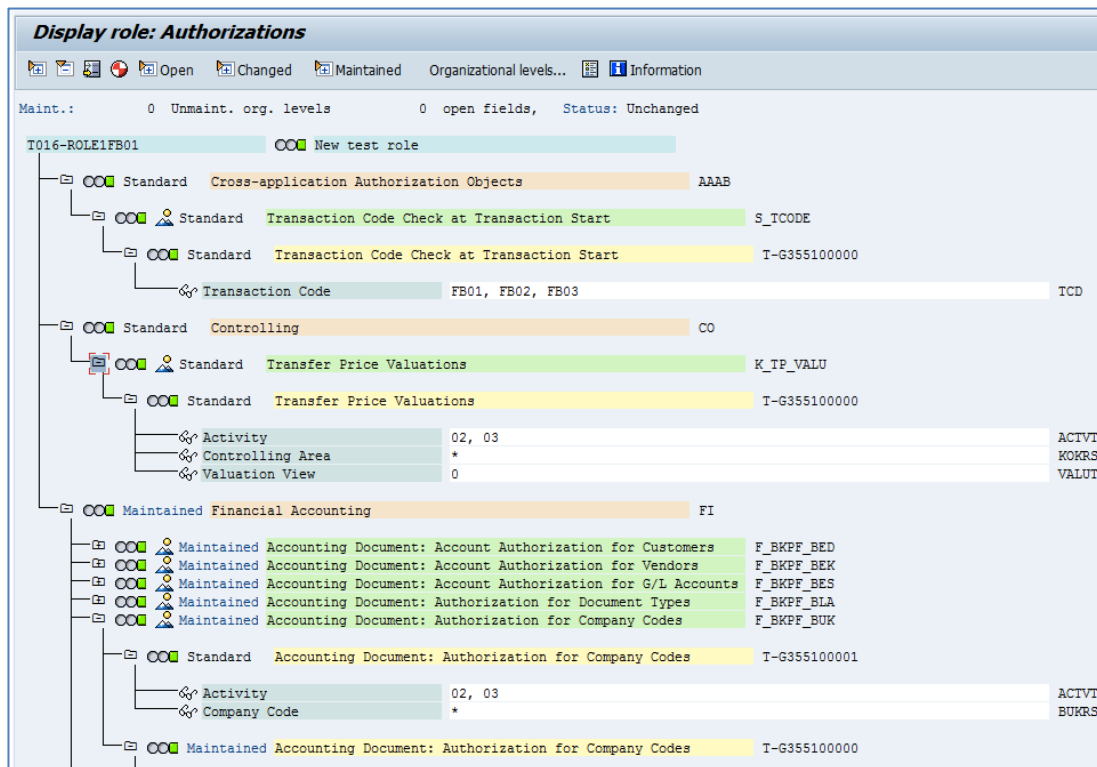
Activities define the actions that can be performed on a transaction or set of transactions in relation to data values. There are almost 200 activity codes in SAP, some very generic and some very specific. For example, 01 (Create or generate), 02 (Change), 03 (Display), 04 (Print, edit messages), 05 (Lock), 06 (Delete), 07 (Activate, generate), 08 (Display change documents), 09 (Display prices) and 10 (Post). For example, you may see that a company code value is tied to an activity code of 02,03 meaning data for that company can be viewed or modified.

The combinations of transactions and other authorization objects are used to define discrete sets of access, mapped to Roles. The following figure shows the relationships.



SAP Roles

The following example is for the role above – T016-ROLE1FB01.



Ignoring the complexity of the SAP display and some levels that aren't important to the discussion, this shows the mapping of a role to the authorization objects.

This role defines a combination of transactions (S_TCODE, in this case FB01, FB02, and FB03), a set of authorization objects for different data values and operations that relate to those transactions.

Different roles with different combinations of transactions and other authorization objects. For example, just looking at some transactions and data AOs (no activities):

Role	Transactions	Company	Bus. Area
T016-ROLE-FBVAR-1	FB01, 02, 03	1000	*
T016-ROLE-FBVAR-2	FB02, 03	1000	*
T016-ROLE-FBVAR-3	FB01, 02, 03	1000-2900	*
T016-ROLE-FBVAR-4	FB01, 02, 03	1000	6000, 7000
T016-ROLE-FBVAR-5	FB03, 04, 05, 07	*	*

These (fabricated) roles are examples to show overlap:

- The first role allows the user to post, change and view a financial document for company 1000 (and any business area).
- The second role is similar but without the ability to post (i.e., can view and change).
- The third role allows the user to post, change and view financial documents for any company in the range 1000-2900.

- The fourth role allows the user to post, change and view a financial document but only for company 1000 and business areas of 6000 or 7000.
- The fifth role allows a number of transactions for any company and business area.

There is access overlap between these roles, and as we will see later, ISVG can highlight issues within roles and between roles.

Note that you cannot map a transaction or other authorization object directly to a user, it must be via a role.

In SAP roles can be:

- Direct Authorizations:
 - Simple roles
 - Imparting roles (Parent)
 - Derived roles
 - Exception roles (no transaction codes inside)
- Indirect Authorizations:
 - Composite roles

There are significant differences in SAP between these. From an ISVG perspective we only see roles (i.e., the direct authorizations) and composite roles (indirect authorizations). The composite role is intended to be a higher-level role, equating to a Job Role (whereas roles may be job functions).

The next sections look at how ISVG can present and analyze these objects from a coarse-grained (enterprise-wide) and fine-grained (SAP-specific) perspective.

Coarse-Grained (Enterprise) Governance

SAP objects loaded via connector reconciliation will contribute to enterprise-wide governance. SAP Users are treated like other accounts and are connected to ISVG Users, SAP Roles become permissions and can be mapped to Business Activities for SoD checks along with other target permissions.

This section is focused on SAP objects pulled directly from SAP via the Connector. There is a slight difference when objects are sync'd from ARCS into ARC which will be covered later.

SAP Objects Loaded

The connector reconcile will create accounts, attempt to match these to ISVG users, create permissions (if not already there) and map them to ISVG users (if the user was found). This uses the normal TARGET queue that all other adapters and connector use. The behavior of the steps can be customized by Java rules associated with the Target queue.

SAP Users in ISVG are like all other accounts and can be viewed via the Manage -> Accounts tab or the Manage -> Users tab.

The SAP Roles are treated like all other roles.

The screenshot shows the IBM Security console interface. On the left, a list of SAP Roles is displayed under the 'Roles' tab. The role 'APO_LC' is highlighted. On the right, the 'Details' panel for 'APO_LC' is shown, including fields for Version (0), Owner, Name (APO_LC), Code (215ea6b6), Description, Type (Permission), Application (GS3), Permission Type (PROFILO), Entitlement Families, Expiration, and Last Review Date (Feb 27, 2016).

ISVG users are connected to SAP Roles during the reconciliation process (or later when unmapped accounts and mapped to users). For example, Maria Becker has a number of SAP Roles (shown as ISVG Permissions – atom icon).

The screenshot shows the 'Users' section of the IBM Security console. A table lists users, with Maria Becker highlighted. To the right, the 'Assigned' permissions for Maria Becker are listed in a table:

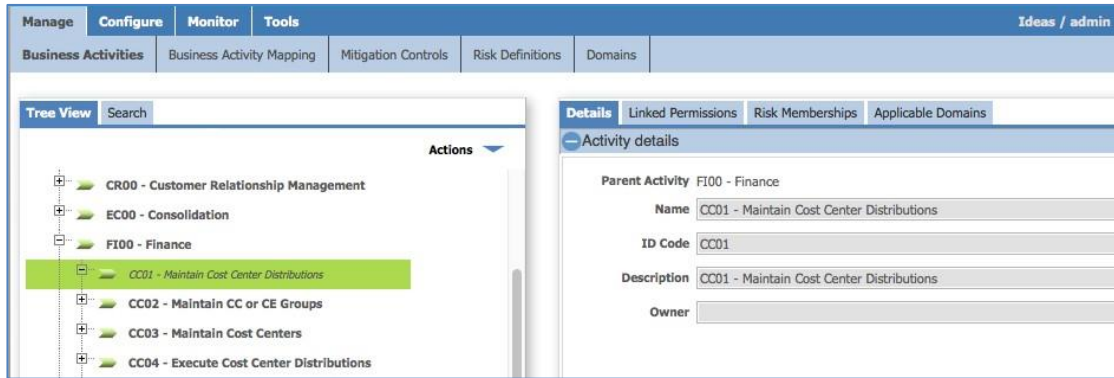
VV	Name	Application	Group Name	Group Code	Hierarchy	Start Date	End Date	Creation Date	Originator
	ZUSESSMENU2	GS3	Sales HFI	50000777	ORGANIZATIONAL_UNIT	Mar 24, 2016 8:58:31 AM			Event Target 21267
	T-000000044	GS3	Sales HFI	50000777	ORGANIZATIONAL_UNIT	Mar 24, 2016 8:58:30 AM			Event Target 21266
	T-000000043	GS3	Sales HFI	50000777	ORGANIZATIONAL_UNIT	Mar 24, 2016 8:58:30 AM			Event Target 21265
	T-000000042	GS3	Sales HFI	50000777	ORGANIZATIONAL_UNIT	Mar 24, 2016 8:58:29 AM			Event Target 21264
	T-000000041	GS3	Sales HFI	50000777	ORGANIZATIONAL_UNIT	Mar 24, 2016 8:58:29 AM			Event Target 21263
	T-00000004	GS3	Sales HFI	50000777	ORGANIZATIONAL_UNIT	Mar 24, 2016 8:58:29 AM			Event Target 21262
	ZZ_RFCACL	GS3	Sales HFI	50000777	ORGANIZATIONAL_UNIT	Feb 27, 2016 1:57:59 PM			Event Target 12467
	R3_BASIC	GS3	Sales HFI	50000777	ORGANIZATIONAL_UNIT	Feb 27, 2016 1:57:59 PM			Event Target 12466
	Z_IDES_ESS	GS3	Sales HFI	50000777	ORGANIZATIONAL_UNIT	Mar 24, 2016 8:06:53 AM			Request:112
	IDESUS_HR_ESS_MENU	GS3	Sales HFI	50000777	ORGANIZATIONAL_UNIT	Feb 27, 2016 1:58:00 PM			Event Target 12468

These permissions can contribute to SoD and SA risks like any other permission.

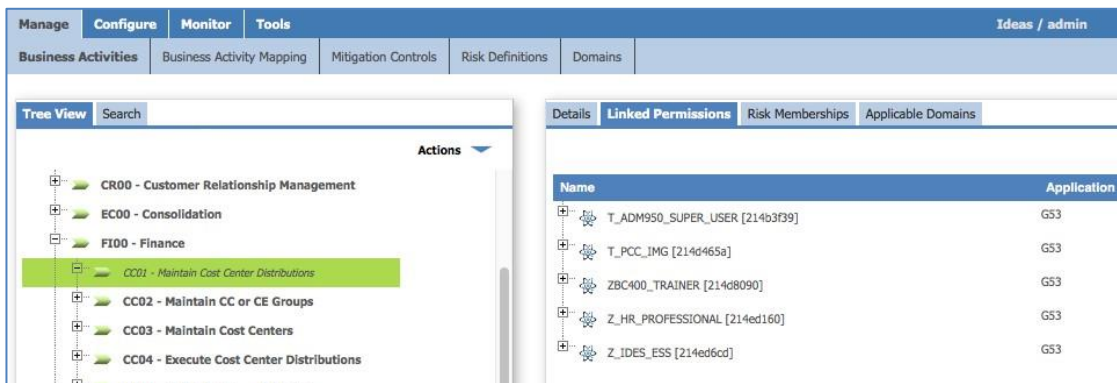
Enterprise SoD

Enterprise risk is defined in the Access Risk Control (ARC). It contains the business activities, BA to permission mapping (linking), the SoD and SA risk definitions and mitigations. This is enterprise-wide, not SAP-specific.

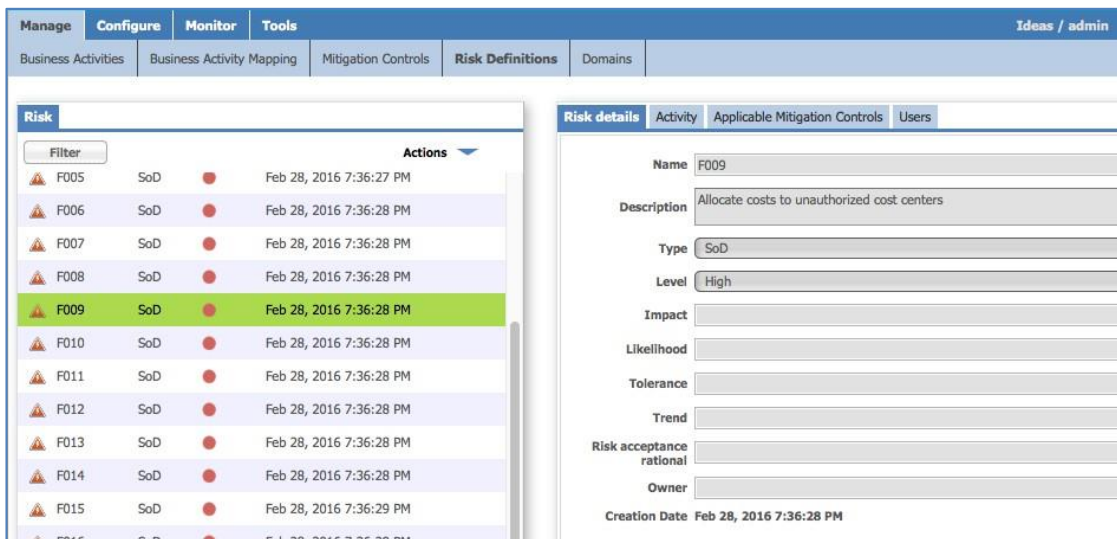
Business activity trees need to be defined, but some are pre-built (like the Financials BAs shown below).



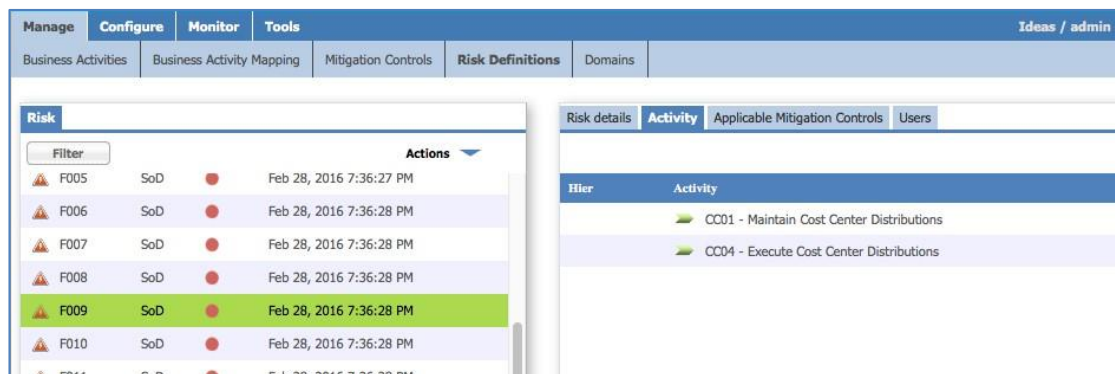
These BAs are linked to SAP permissions or other target system permissions.



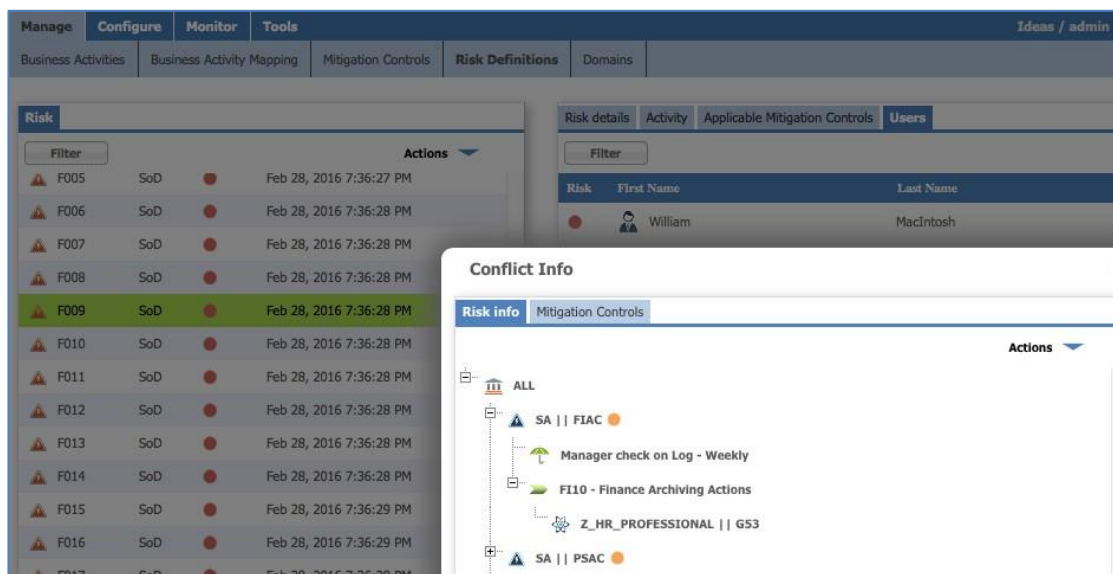
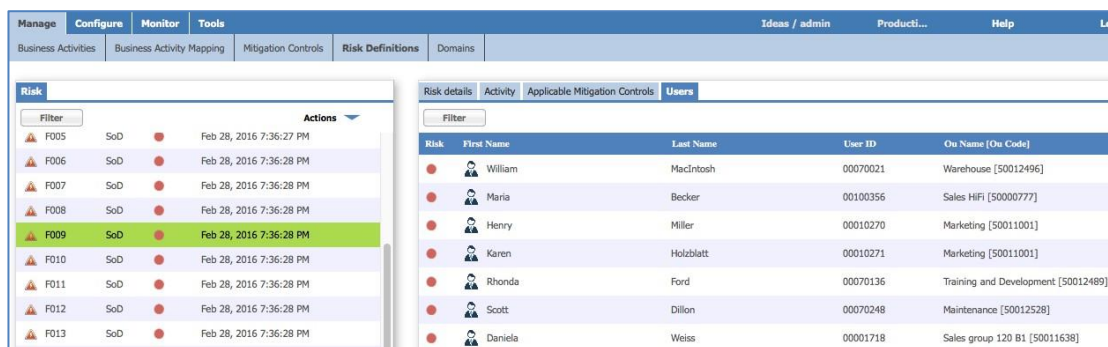
The risk definitions will be either Separation of Duties (SoD) or Sensitive Access (SA).



They will map to Business Activities.



We can see the users associated with a risk and the details of the risks associated with a user.



In this example we can see Wilson MacIntosh is carrying multiple risks that include a Medium level sensitive access risk of “FIAC” which is tied to the “FI10 – Finance Archiving Action” business activity. The FI10 business activity includes the Z_HR_PROFESSIONAL SAP Role which Wilson MacIntosh has.

The risks may be across a single SAP Role, between SAP Roles, or between SAP Roles and permissions for other target systems. Because many SAP roles contain a complex set of permissions (transactions and other authorization objects) we need to use the fine-grained SAP module (ARCS) to identify SAP Roles that contain risk within their definitions.

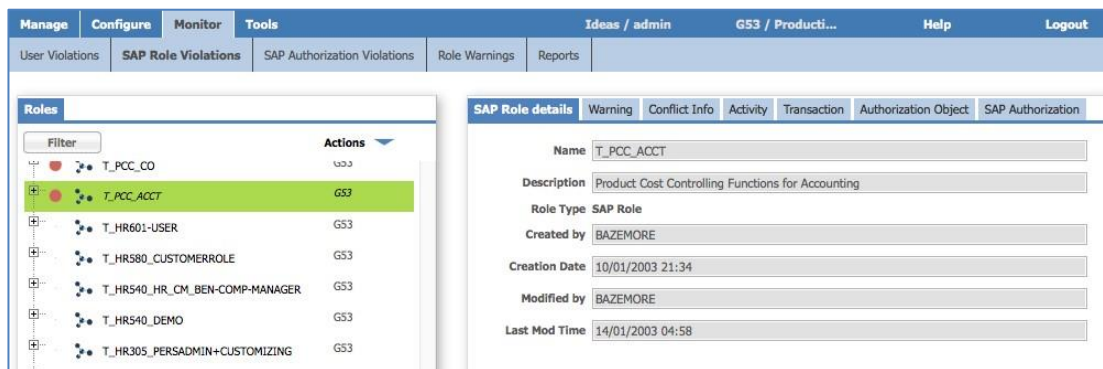
Fine-Grained (SAP-Specific) Governance

The Access Risk Control for SAP (ARCS) module is dedicated to analyzing risk associated with SAP Roles, the transactions and other authorization objects the roles contain. It is similar to the enterprise-wide Access Risk Controls (ARC) module, and many of the concepts (business activities, SoD/SA risk, BA mapping) are the same, but there are some differences. This section explores the use of the ARCS module for understanding SAP risk.

The ARCS module will use users and SAP Roles loaded via the SAP Connector (or other means like a bulk load or one of the ISIM Provisioning Adapters), business activities and risks from ARC, and fine-grained objects collected from SAP via the SAP Connector Agent. We will look at where the data comes from in a later section.

SAP Authorization Objects in ISVG

The Load process will consume all SAP Roles, transactions, authorization objects and relationships. The following figure shows a SAP Role (“T_PCC_ACCT”) in ARCS.



The screenshot displays the ISVG interface with the 'SAP Role details' tab selected. The role 'T_PCC_ACCT' is highlighted in the Roles list on the left. The details panel on the right shows the following information:

Name	T_PCC_ACCT
Description	Product Cost Controlling Functions for Accounting
Role Type	SAP Role
Created by	BAZEMORE
Creation Date	10/01/2003 21:34
Modified by	BAZEMORE
Last Mod Time	14/01/2003 04:58

The following figure shows the transactions mapped to the role.



The screenshot displays the ISVG interface with the 'Transaction' tab selected under 'SAP Role details'. The role 'T_PCC_ACCT' is still highlighted in the Roles list on the left. The transactions table is as follows:

Transaction Group	Name	Description
FSIB	FSIB	
F110	F110	
FB60	FB60	
FK01	FK01	
FK06	FK06	
S_ALR_87012082	S_ALR_87012082	
S_ALR_87012086	S_ALR_87012086	
S_ALR_87012103	S_ALR_87012103	

Similarly, we can see the authorization objects mapped to the role.

The screenshot shows the SAP Role configuration interface. On the left, a list of roles is displayed under the 'Roles' tab, with 'T_PCC_ACCT' selected. On the right, the 'SAP Role details' tab is active, showing a table of authorization objects (AOs) for the selected role.

Auth Object	AO description	SAP Auth	Field Name	Min	Max
A_A_VIEW		T-1355012100	VIEW	*	
A_A_VIEW		T-1355012101	VIEW	1	2
A_B_ANLKL		T-1355012100	ACTVT	01	
A_B_ANLKL		T-1355012100	ACTVT	02	
A_B_ANLKL		T-1355012100	ACTVT	03	
A_B_ANLKL		T-1355012100	ACTVT	77	
A_B_ANLKL		T-1355012100	ANLKL	*	
A_B_ANLKL		T-1355012101	ACTVT	*	
A_B_ANLKL		T-1355012101	ANLKL	*	
A_B_BWART		T-1355012100	ANLKL	*	
A_B_BWART		T-1355012100	BWASL	*	
A_B_BWART		T-1355012101	ANLKL	*	
A_B_BWART		T-1355012101	BWASL	100	
A_PERI_BUK		T-1355012100	AM_ACT_PER	30	

Note that the authorization objects are not tied to specific transactions. The authorization objects have their own fields and values that may apply to one or more transactions depending on what AOs apply to each transaction.

For example, the A_A_VIEW AO has two set of values in the role; one that restricts values to the range 1-2 (i.e., one or two) and one that has a wildcard. There is an obvious conflict here.

This role has 1067 transactions and 865 authorization objects mapped to it. It is a huge and complex role has could have many conflicting accesses contained within it.

We can also see collective roles in ISVG, including the roles that make up the collective role. For example:

The screenshot shows the SAP Role configuration interface. On the left, a list of roles is displayed under the 'Roles' tab, with 'Z_SCM310' selected. On the right, the 'SAP Role details' tab is active, showing a form for the selected role.

SoD	Name	Application
	Z_SCM310	G53
	SAP_EPM_PLANT_MANAGER	G53
	Z_SCM310_SFC	G53
	CC07-K088	G53
	Z_SAP_AUDITOR_TAX	G53

The 'SAP Role details' form shows the following information:

- Name: Z_SCM310
- Description: [Empty field]
- Role Type: Collective Role
- Created by: [Empty field]
- Creation Date: [Empty field]
- Modified by: [Empty field]
- Last Mod Time: [Empty field]

The user to permission (i.e., ISVG user to SAP Role) relationships are available in the identity warehouse and accessed by the ARCS module. If you don't load this information (e.g., bulk load or using the SAP Connector) you won't see the user-based information in ARCS.

ISVG SAP Authorization Patterns (or Risk Entitlements)

In ISVG we use the Business Activity model to define risk. Business activities (such as "purchase order create" and "purchase order approve") define job functions that may be part of a job role. Risks may be separation of duties (or toxic combinations) between business activities or sensitive access (like privileged access) for a specific business activity.

As well as defining the risks (SoD and SA) we also need to define what permissions for a specific deployment map to the business activities (e.g., what application group/role/transaction implements the “purchase order create” function in Company XYZ).

[The Problem with SAP Roles for BA Mapping](#)

For SAP it’s natural to think we can use SAP Roles to map to business activities (in the same way that we would map an AD Group or a RACF CICS Transaction to a BA). However, as we saw in the previous section, SAP Roles may be large and complex, covering many transactions and authorization objects with potential for overlap and unexpected access decisions. This is fine if we want to identify users with risk through their roles, but not good if we want to understand the risk inherent in a role and perform some role cleanup.

We need a more granular definition of access in SAP that we can tie to business activities.

In ISVG we have the construct of “SAP Authorizations” or “SAP Authorization Patterns” (previously known as “SAP Risk Entitlements”).

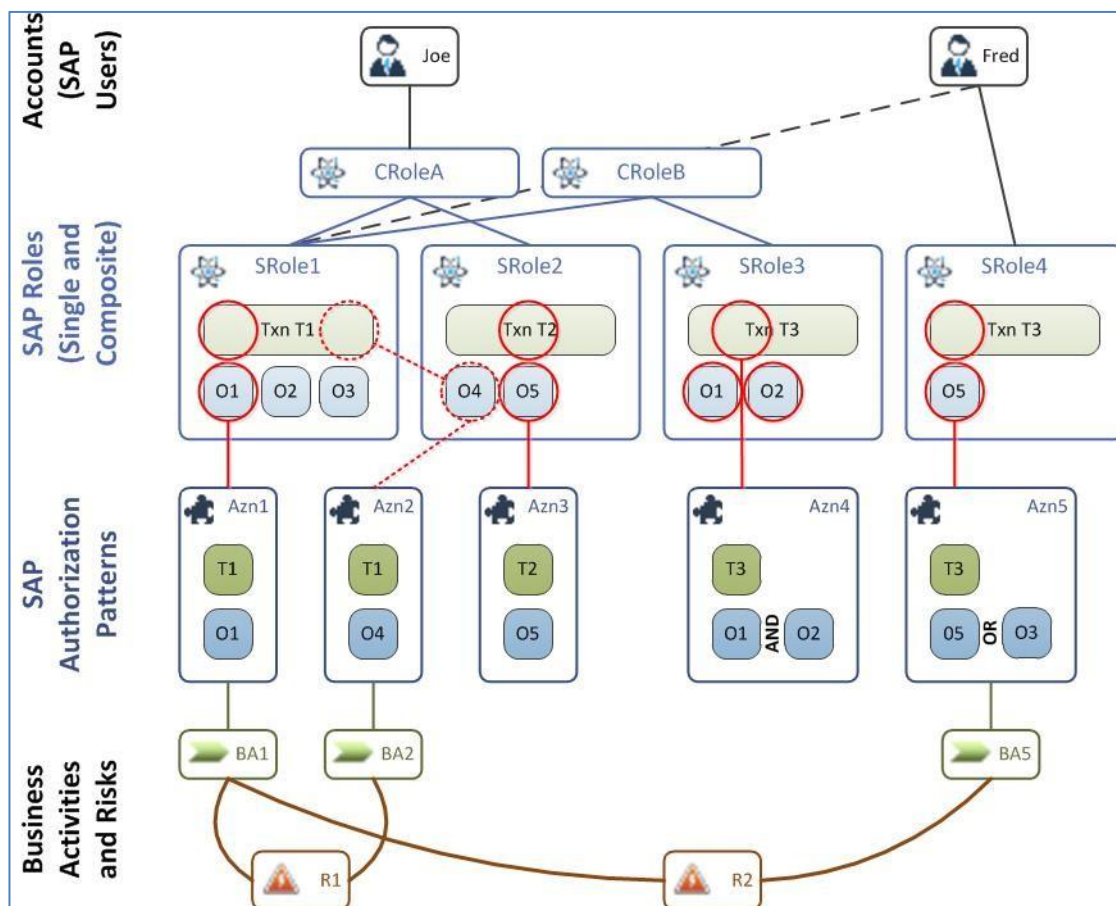
[SAP Authorization Patterns](#)

A SAP Authorization Pattern is a combination of one or more AOs for a specific transaction that are granular enough to map to a business activity.

If a SAP Role is tied to a single transaction with a small set of AOs, then the SAP Authorization Pattern may be equal to the SAP Role. In most cases there may be many SAP Authorization Patterns that cover part of a SAP Role.

[SAP Roles and SAP Authorization Patterns](#)

The following figure provides an example of data objects and how they come together to provide the governance picture.



Let’s start with the SAP Roles. There are four single roles shown with different combinations of transactions and authorization objects.

- SRole1 (T1, O1, O2, O3)
- SRole2 (T2, O4, O5)
- SRole3 (T3, O1, O2)
- SRole4 (T3, O5)

We have defined five SAP Authorization Patterns:

- Azn1 (T1, O1)
- Azn2 (T1, O4)
- Azn3 (T2, O5)
- Azn4 (T3, O1 AND O2)
- Azn5 (T3, O5 OR O3)

These five Authorization Patterns may represent unique functions in SAP (combination of transaction and authorization objects) that could be a potential risk in the SAP system or granular functions we want to provide governance visibility to.

The figure shows how the SAP Authorization Patterns map to the SAP Roles. Authorization Patterns Azn1, Azn2, Azn3 and Azn4 map to SRole1, SRole2, SRole3 and SRole4, respectively. There could be multiple Authorization Patterns mapping to a single Role, or a single Authorization Pattern could be found in multiple roles.

The patterns Azn4 and Azn5 show how there may be a need to combine AOs for a transaction to define the needed level of granularity. Azn4 has T3 and O1 AND O2, so for it to be matched to a role, both AOs must be present (like in SRole3). Azn5 has T3 and O5 OR O3, so for it to be matched to a role either combination (T3+O4 or T3+O5) must be found (like in SRole4).

Notice that the SAP Authorization Pattern Azn2 does not cover a role completely – the transaction is in SRole1 and the AO is in SRole2. So, a single role does not map to the Authorization Pattern. However, if the roles are combined, either through a Composite Role (like CRoleA) or because a user is connected to both SRole1 and SRole2, SAP will merge the transactions and authorization objects and so Azn2 will be valid. This is often referred to as cross-contamination of roles – two roles when combined present unexpected access.

The diagram shows three business activities mapped to three of the SAP Authorization Patterns:

- BA1 -> Azn1 (T1, O1)
- BA2 -> Azn2 (T1, O4)
- BA5 -> Azn5 (T3, O5)

These business activities are also tied to SoD Risks.

- R1 has BA1 and BA2
- R2 has BA1 and BA5

How does this affect users? If we have a user Fred who is in Role SRole5. The Authorization Pattern Azn5 is found in role SRole5, so Fred has the business activity BA5 but no risk violations. If we then add Fred to SRole1 he then has business activity BA1 (through the Authorization Pattern Azn1 in role SRole1). This triggers the SoD Risk R2.

How about user Joe. He's in the composite role CRoleA. This consists of SRole1 and SRole2. The Authorization Patterns that apply to Joe are Azn1 (from SRole1), Azn3 (from SRole2) and Azn2 (from SRole1+SRole2). Azn1 is mapped to BA1, and Azn2 is mapped to BA2, and these two BAs comprise SoD Risk R1. The composite role CRoleA contains the SoD violation, so any user (like Joe) that is mapped to the role will also be in violation.

The ARCS module, using the SAP Authorization Patterns, allows both role- and user-based risk to be identified.

An Example of SAP Roles and SAP Authorization Patterns in ISVG

The following figure shows a role (T_PCC_ACCT) and the SAP Authorizations mapped to it.

Name	Functionality Type	Application
GL03-FB41	SAP_AUTHORIZATION	G53
GL03-F-42	SAP_AUTHORIZATION	G53
GL03-F-21	SAP_AUTHORIZATION	G53
GL03-F13E	SAP_AUTHORIZATION	G53
GL03-F101	SAP_AUTHORIZATION	G53
GL03-F-05	SAP_AUTHORIZATION	G53
GL03-F.38	SAP_AUTHORIZATION	G53
GL03-F.14	SAP_AUTHORIZATION	G53
GL03-F.13	SAP_AUTHORIZATION	G53
GL03-F.05	SAP_AUTHORIZATION	G53

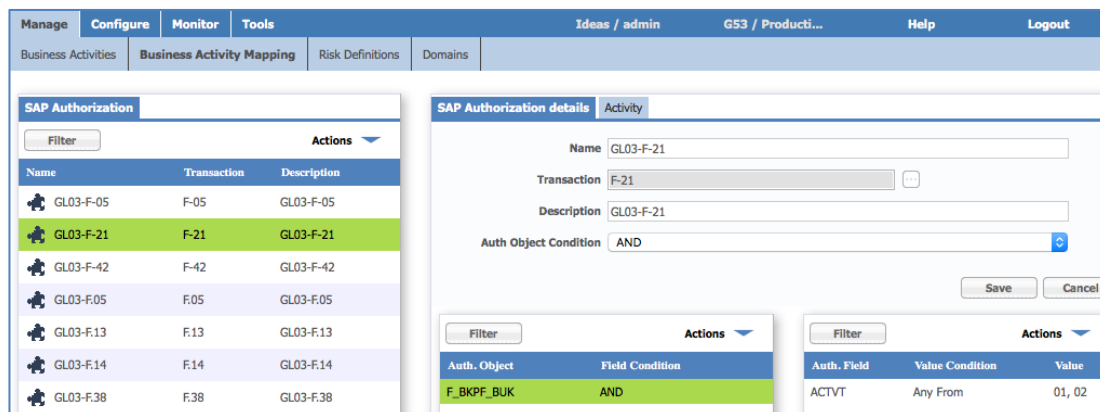
There are actually 98 SAP Authorization Patterns found in the SAP Role T_PCC_ACCT. The following figures show the SAP Authorization Patterns GL03-FB41, GL03-F-42 and GL03-F-21.

Name	Transaction	Description
GL03-FBWE	FBWE	GL03-FBWE
GL03-FBBCX	FBBCX	GL03-FBBCX
GL03-FBB1	FBB1	GL03-FBB1
GL03-FB41	FB41	GL03-FB41
GL03-FAGL_FC_VAL	FAGL_FC_VAL	GL03-FAGL_FC_VAL
GL03-FAGL_FC_TRANS	FAGL_FC_TRANS	GL03-FAGL_FC_TRANS
GL03-FAGLF101	FAGLF101	GL03-FAGLF101

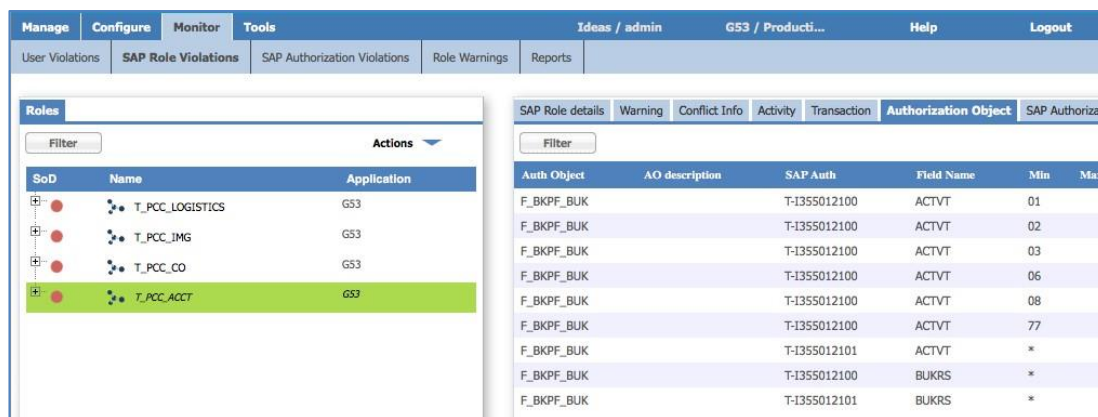
Auth. Object	Field Condition
F_BKPF_BUK	AND

Name	Transaction	Description
GL03-F-05	F-05	GL03-F-05
GL03-F-21	F-21	GL03-F-21
GL03-F-42	F-42	GL03-F-42
GL03-F.05	F.05	GL03-F.05
GL03-F.13	F.13	GL03-F.13
GL03-F.14	F.14	GL03-F.14
GL03-F.38	F.38	GL03-F.38
GL03-F101	F101	GL03-F101

Auth. Object	Field Condition
F_BKPF_BUK	AND



Each SAP Authorization Pattern maps to a single transaction (FB41, F-42, and F-21) and each one has a single field for the F_BKPF_BUK (“Accounting Document: Authorization For Company Codes”) AO with activity codes (operations) of 01, 02 (add, modify). They map to the role because the role has those transactions and authorization objects.



Each of these AOs is mapped to the business activity of “GL03 – Post Journal Entry (misc Tax/Currency).” This mapping and the risk analysis it allows is covered in the next section.

Defining SAP Risk in ARCS

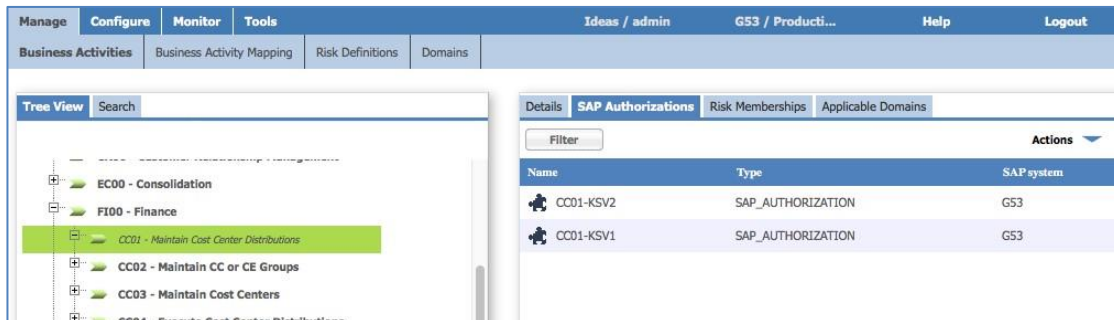
Now that we understand the SAP Authorization Patterns that ISVG uses, and how they are tied to SAP Roles from the SAP system, we can look at how we manage risk.

Business Activities and Mapping in ARCS

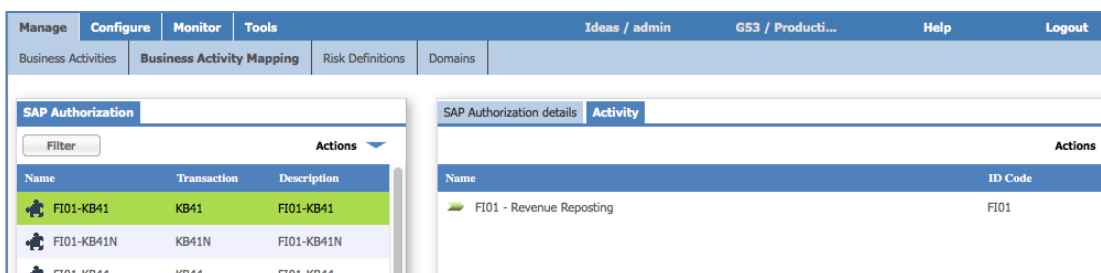
Whereas in the enterprise-wide risk module (ARC) we mapped business activities to permissions, in ARCS we map business activities to SAP Authorization Patterns.

Thus, an ISVG User will belong to a business activity because their SAP account is mapped to a SAP Role, and that role is mapped to a SAP Authorization Pattern, and that SAP Authorization Pattern is mapped to a business activity.

The risk definitions are built on business activities as they are in ARC. SAP Authorization Patterns mapped to business activities can be viewed/added/removed from the Business Activities tab in ARCS.



Activities can also be added to/removed from the SAP Authorization from the Business Activity Mapping tab in ARCS.

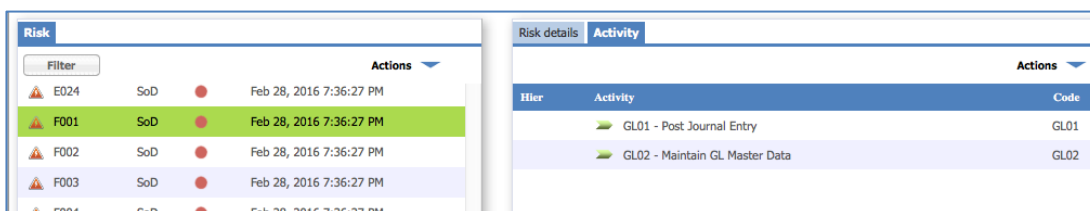
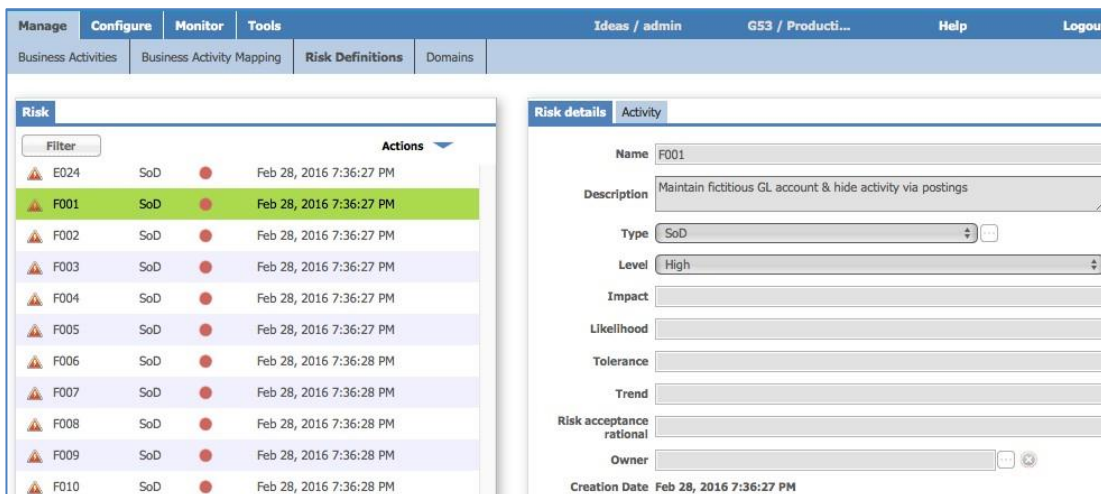


The Business Activity Mapping tab is also the place to manually define SAP Authorizations. They can also be bulkloaded from XLS files under the Tools menu.

Risks in ARCS

Risks in ARCS are defined in exactly the same way as risks in ARC. The Risk Definitions tab in ARCS allows for creation/modification/deletion of risks.

For example:



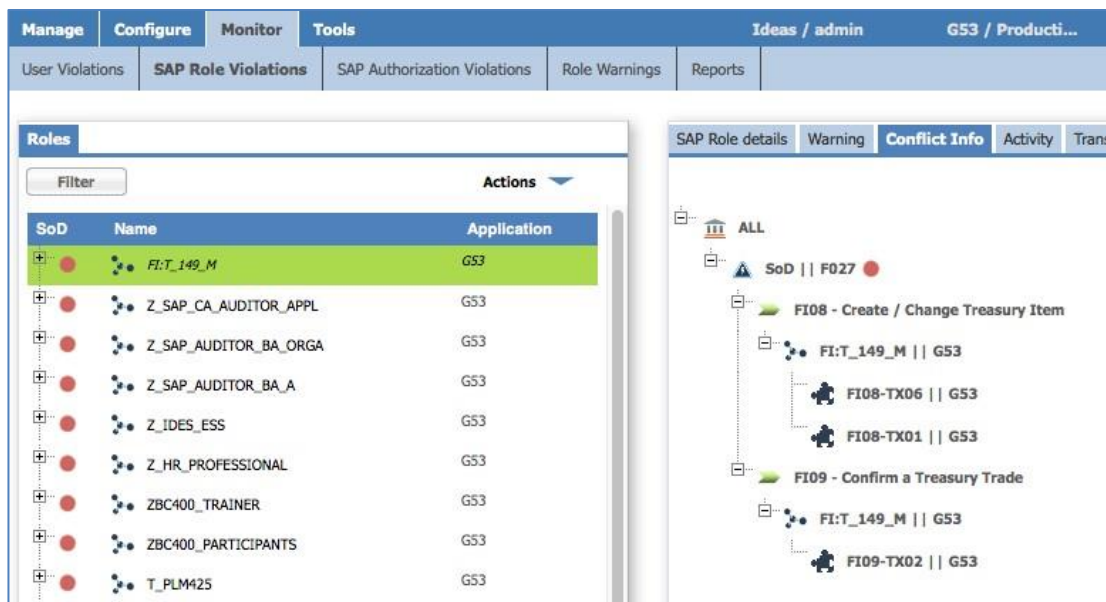
This shows a High-level SoD Risk, F001, that has two business activities: GL01 – Post Journal Entry and GL02 – Maintain GL Master Data.

With the risks defined, we can look at the violations that ARCS can report on.

SAP Role Violations

The “SAP Role Violations” view shows SAP Roles that contain risks due to the SAP Authorization Patterns corresponding.

The view shows all Roles and highlights the ones with risk (colored dot, as used throughout ISVG). For example, the SAP Role FI:T_149_M contains a single SoD violation.



SoD	Name	Application
●	FI:T_149_M	G53
●	Z_SAP_CA_AUDITOR_APPL	G53
●	Z_SAP_AUDITOR_BA_ORGA	G53
●	Z_SAP_AUDITOR_BA_A	G53
●	Z_IDES_ESS	G53
●	Z_HR_PROFESSIONAL	G53
●	ZBC400_TRAINER	G53
●	ZBC400_PARTICIPANTS	G53
●	T_PLM425	G53

The detailed view shows the SoD violation F027, which includes the following business activities and mappings:

- FI08 - Create / Change Treasury Item
 - FI08-TX06 || G53
 - FI08-TX01 || G53
- FI09 - Confirm a Treasury Trade
 - FI:T_149_M || G53
 - FI09-TX02 || G53

The SoD violation is “F027” which comprises the business activities of “FI08 – Create / Change Treasury Item” and “FI09 – Confirm a Treasury Trade”. This means that someone with this role could add a trade and approve it, an obvious SoD violation.

The “FI08 – Create / Change Treasury Item” business activity is mapped to the FI08-TX06 and FI08-TX01 SAP Authorizations. The “FI09 – Confirm a Treasury Trade” business activity is mapped to the FI09-TX02 SAP Authorization.

As the SAP Role has transactions and AOs that correspond with these three SAP Authorization Patterns, then the role contains the conflict. This is similar to having a Business Role in ISVG that contains multiple permissions mapped to conflicting business activities, thus the role itself contains conflicts.

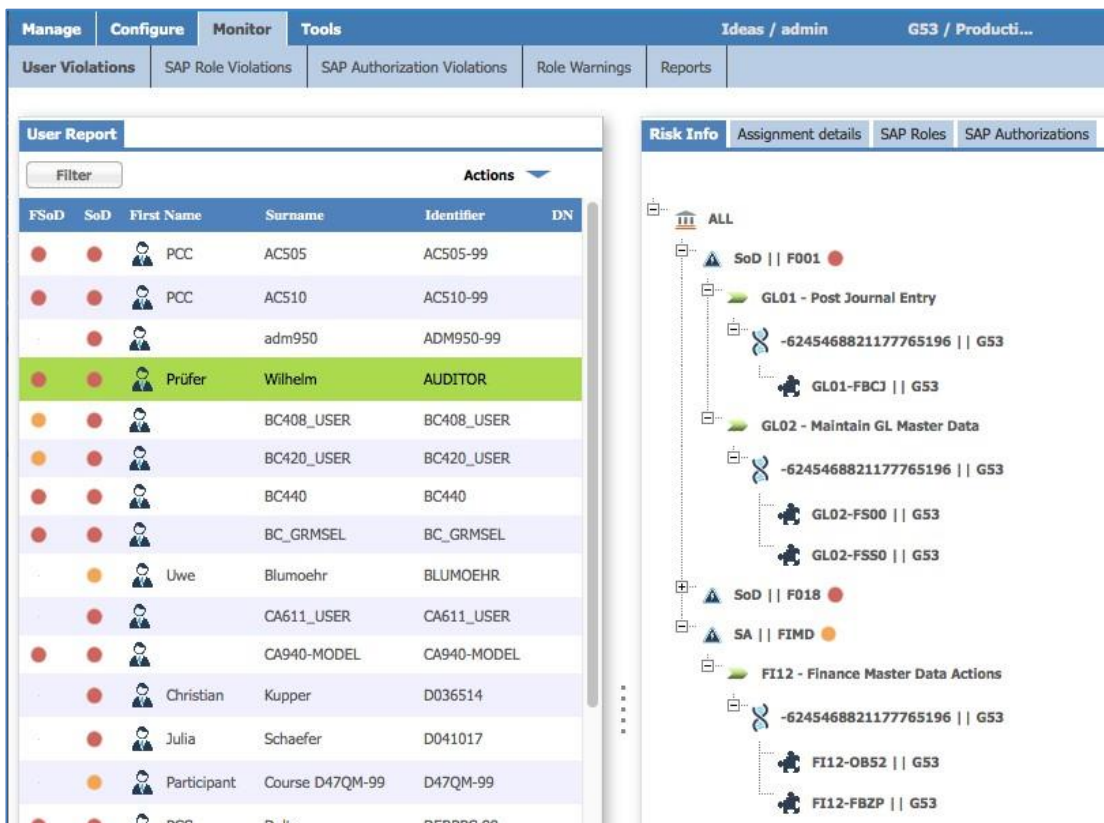
SAP Authorization Violations

It may be that the SAP Authorization Patterns that have been defined represent conflict themselves. For example, maybe the same SAP Authorization Pattern is mapped to two different business activities that comprise a SoD rule. That may be unavoidable as the one transaction could be used for conflicting activities.

User Violations

The “User Violations” view shows users that have conflicts, due to the roles they have.

The following figure shows users that contain conflicts.



FSoD	SoD	First Name	Surname	Identifier	DN
●	●	PCC	AC505	AC505-99	
●	●	PCC	AC510	AC510-99	
●	●	adm950		ADM950-99	
●	●	Prüfer	Wilhelm	AUDITOR	
●	●	BC408_USER		BC408_USER	
●	●	BC420_USER		BC420_USER	
●	●	BC440		BC440	
●	●	BC_GRMSEL		BC_GRMSEL	
●	●	Uwe	Blumoehr	BLUMOEHR	
●	●	CA611_USER		CA611_USER	
●	●	CA940-MODEL		CA940-MODEL	
●	●	Christian	Kupper	D036514	
●	●	Julia	Schaefer	D041017	
●	●	Participant	Course D47QM-99	D47QM-99	
●	●	PCC	Delta	DERPBC-99	

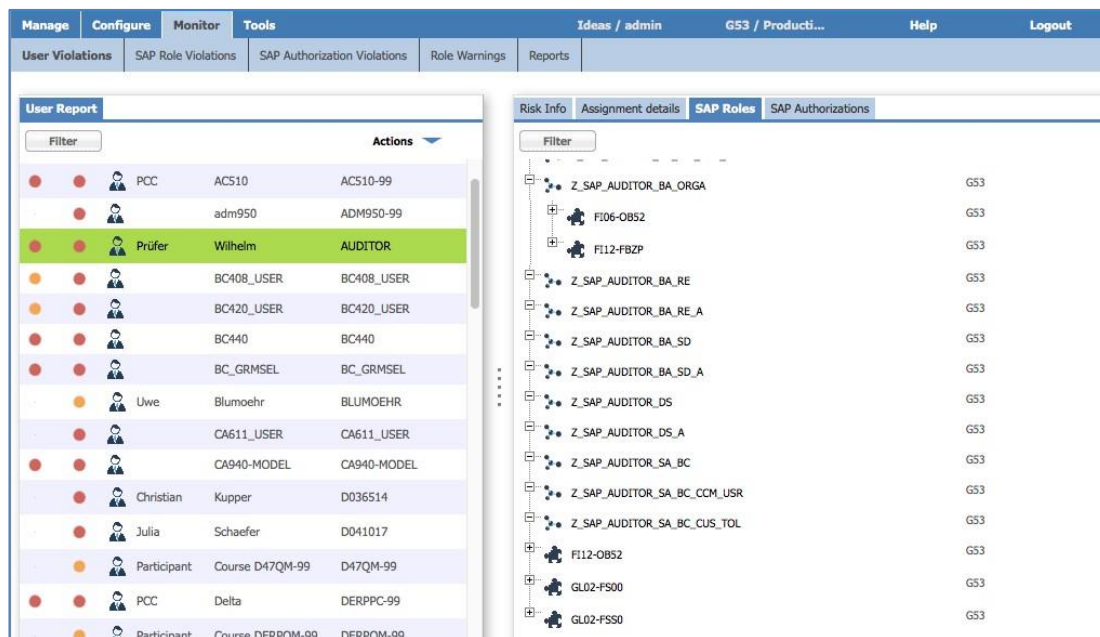
The highlighted user, Prüfer Wilhelm, has two SoD and one SA risks. Notice that there are two risk ratings shown and that the risks seem to have randomly generated negative numbers instead of names.

The User Report shows two types of SoD violation:

- SOD (Traditional SoD) – business activities in conflict mapped to two SAP Authorization Patterns within a SAP Role.
- FSoD (Cross-contamination), Full SoD – unintended overlap of AO between two roles representing unexpected access

To determine cross-contamination risks, ARCS must build combined definitions and that is what the collective roles (blue double-helix icon) with the negative random number labels represent.

Let’s look at the FIMD SA violation. It is mapped to two SAP Authorization Patterns: FI12-OB52 and FI12-FBZP. We can look at the SAP Roles mapped to Prüfer Wilhelm, and the SAP Authorization Patterns that correlate to them.



The Z_SAP_AUDITOR_BA_ORGO role correlates to the FI12-FBZP SAP Authorization Pattern. But no other SAP Roles correlate to FI12-OB52. However, it is listed at the bottom (not belonging to any Role).

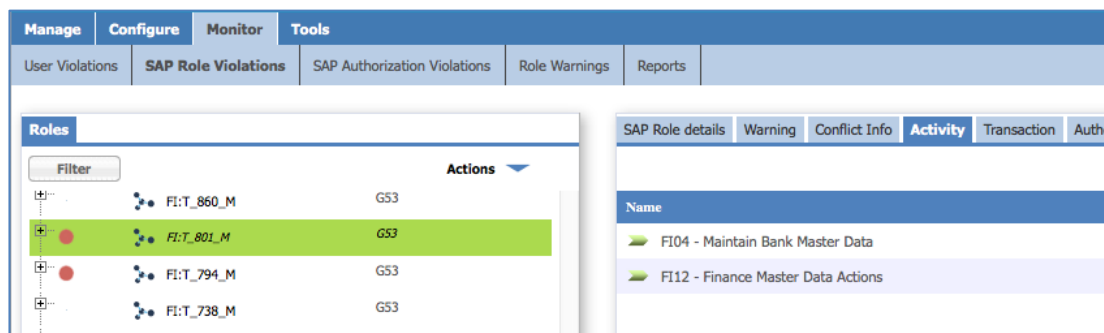
This means the ARCS module has determined that across a number of SAP Roles belonging to this user, there is the right combination of transaction(s) and AOs that correspond to the FI12-OB52 SAP Authorization Pattern, and this tied to the SA violation.

This is very powerful and shows that even though a single role might not cause a violation, there may be combinations of roles providing an unexpected cross-contamination of access.

How Well are the Roles Named?

One of the positive benefits of using the business activities model and mapping them to SAP Authorization Patterns is that we can get a good view of how well the roles are named.

For example, we can look at a role cryptically named FI:T_801_M as follows.



Because of the SAP Authorization Patterns found in the role definition, and because those SAP Authorization Patterns are mapped to business activities, we can get a reasonable understanding of what the role covers (e.g., Maintain Bank Master Data and Finance Master Data Actions).

ISVG ARCS could be used as a tool to help renaming of roles, or at least applying some sort of description to the roles to make access requests and certification more business-user friendly.

Role Warnings (Bad Practice Analysis for SAP Access Control Model)

The “Role Warnings” view is a result of analysis run against the authorization data pulled from SAP. It does not involve the normal ARCS risk analysis and SAP Authorization Patterns – it is merely looking for known bad practices in the authorization data.

The patterns it is looking for are:

- Roles without any transactions mapped,
- Roles without authorization objects mapped, and
- Roles with wildcarded (“starred”) transactions.

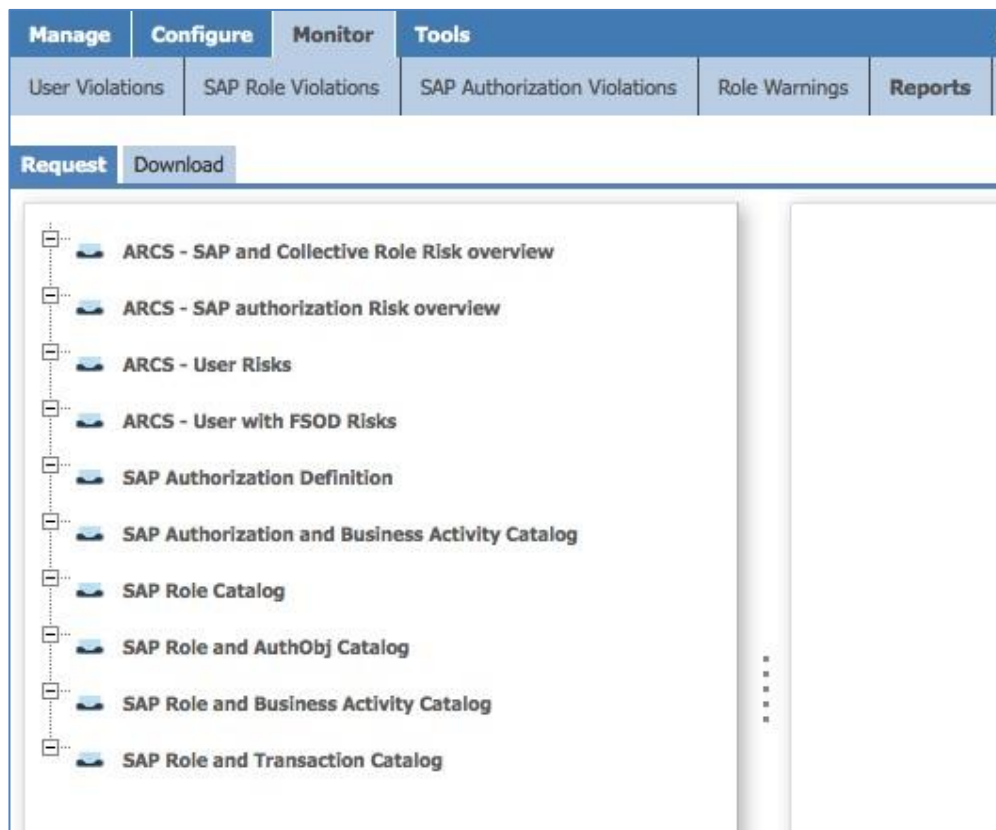
An example of this report is shown below.

Manage	Configure	Monitor	Tools	Ideas / admin	G53 / Producti...	Help	Logout
User Violations	SAP Role Violations	SAP Authorization Violations	Role Warnings	Reports			
Warnings View							
Filter							Actions
Role	Role description	Code	Severity	Description			
/ERPSOLUT/EXTERNAL_CANDIDATE	External Candidate in E-Recruiting	w/o T	Low	role without transaction			
/ERPSOLUT/UNREGISTERED_CAND	Non Registered Candidate (Service User) in E-Recruiting	w/o T	Low	role without transaction			
AAA_ROLESWITCH	The workplace and user settings are updated automatically.	w/o AO	Low	role without Auhtorizable Object			
AUTOID21_ALL	AUTOID21_ALL	w/o T	Low	role without transaction			
BC:E_801_M	GRC - SPM - Admin	w/o T	Low	role without transaction			
BC:T_004_M	e rielaborabile manualmente	w/o AO	Low	role without Auhtorizable Object			
BC:T_033_M	Blocco transazioni - M	w/o AO	Low	role without Auhtorizable Object			
BC:T_040_M	Monitor RFC - M	w/o AO	Low	role without Auhtorizable Object			
BC:T_048_E	e rielaborabile manualmente	w/o AO	Low	role without Auhtorizable Object			
BC:T_201_V	Report per Certificatori e Focal Point	w/o AO	Low	role without Auhtorizable Object			
CA940_DISPLAY	- PA*: HR transactions	T*	High	role with star transaction			
CA:T_002_V	Anagrafico delle Modifiche - V	w/o AO	Low	role without Auhtorizable Object			
CA:T_801_M	e rielaborabile manualmente	w/o AO	Low	role without Auhtorizable Object			

It is possible to add more Java code to this report to identify other bad practices.

SAP-specific Reporting in ISVG

ARCS provides a number of SAP-specific reports.



The reporting mechanism is the same as for the other modules in ISVG – you select the report, specify arguments and output format, and submit. The report is produced in the background.

The following is an example of the ARCS – SAP and Collective Role Risk overview report in XLS.

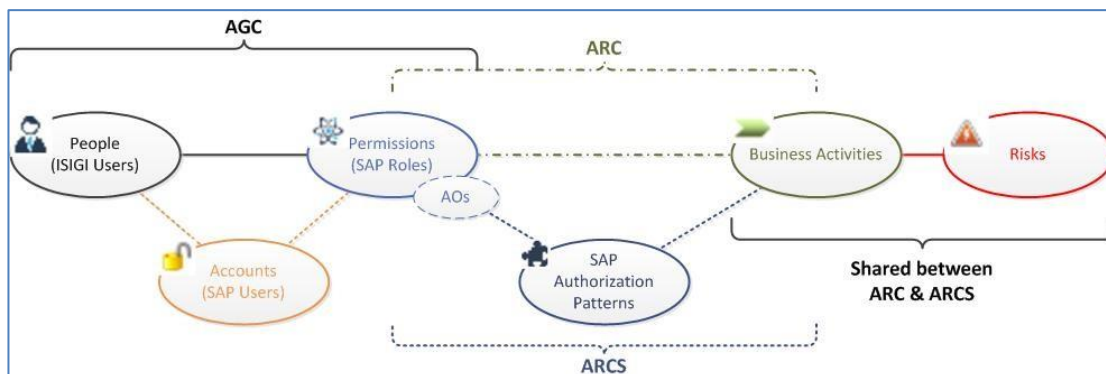
SAP System	Entitlement Name	Entitlement Descr.	Entitlement Type	SAP Authorization	U	D	o	Activity Name	AC	Risk Name	Risk Type	Risk Severity
G53	CO:T_043_M	e ri elaborabile manualmente	SAP Role	CC01-KSV1	A			CC01 - Maintain Cost Center Distributions	C	F009	SoD	HIGH
G53	T_ADM950_SUPER_USER		SAP Role	CC01-KSV1	A			CC01 - Maintain Cost Center Distributions	C	F009	SoD	HIGH
G53	T_PCC_IMG	Manually added OKG4, CPT1 and KZS2	SAP Role	CC01-KSV1	A			CC01 - Maintain Cost Center Distributions	C	F009	SoD	HIGH
G53	ZBC400_TRAINER	Berechtigungen für ABAP-Trainer BC400, etc	SAP Role	CC01-KSV1	A			CC01 - Maintain Cost Center Distributions	C	F009	SoD	HIGH
G53	Z_HR_PROFESSIONAL	Human Resources Professional	SAP Role	CC01-KSV1	A			CC01 - Maintain Cost Center Distributions	C	F009	SoD	HIGH
G53	Z_IDES_ESS	T 50013222 Standard IDES	SAP Role	CC01-KSV1	A			CC01 - Maintain Cost Center Distributions	C	F009	SoD	HIGH
G53	CO:T_043_M	e ri elaborabile manualmente	SAP Role	CC01-KSV2	A			CC01 - Maintain Cost Center Distributions	C	F009	SoD	HIGH
G53	T_ADM950_SUPER_USER		SAP Role	CC01-KSV2	A			CC01 - Maintain Cost Center Distributions	C	F009	SoD	HIGH
G53	T_PCC_IMG	Manually added OKG4, CPT1 and KZS2	SAP Role	CC01-KSV2	A			CC01 - Maintain Cost Center Distributions	C	F009	SoD	HIGH
G53	ZBC400_TRAINER	Berechtigungen für ABAP-Trainer BC400, etc	SAP Role	CC01-KSV2	A			CC01 - Maintain Cost Center Distributions	C	F009	SoD	HIGH
G53	Z_HR_PROFESSIONAL	Human Resources Professional	SAP Role	CC01-KSV2	A			CC01 - Maintain Cost Center Distributions	C	F009	SoD	HIGH
G53	Z_IDES_ESS	T 50013222 Standard IDES	SAP Role	CC01-KSV2	A			CC01 - Maintain Cost Center Distributions	C	F009	SoD	HIGH
G53	T_ADM950_SUPER_USER		SAP Role	CC02-KAH1	A			CC02 - Maintain CC or CE Groups	C	F004	SoD	HIGH
G53	T_ADM950_SUPER_USER		SAP Role	CC02-KAH1	A			CC02 - Maintain CC or CE Groups	C	F023	SoD	HIGH
G53	T_PCC_CO	object, to allow postings.	SAP Role	CC02-KAH1	A			CC02 - Maintain CC or CE Groups	C	F004	SoD	HIGH
G53	T_PLM410	Course PLM410 - "Quality Notification"	SAP Role	CC02-KAH1	A			CC02 - Maintain CC or CE Groups	C	F004	SoD	HIGH

As with the other modules custom reports can be developed, either from scratch or based off an existing report.

Where Does All the Data Come from?

There are many data sets that need to be present to use the SAP functionality discussed in this section.

The following figure shows the key data objects and their relationships.



Within Access Governance Core we focus on People, their Accounts and Permissions. When an account is loaded, it is matched to a user and any account-permission membership becomes a Person-Permission mapping.

In both Access Risk Control modules (ARC and ARCS) we define Business Activities and these business activities are mapped to Risks (e.g., SoD or SA).

In ARC (sometimes called the “Enterprise Realm”) business activities are mapped to permissions. In ARCS this is more complicated; SAP Authorization Patterns are associated with the permissions (SAP Roles) where the transactions and authorization objects match, and SAP Authorization patterns are mapped to business activities.

Thus, the data we need to load into ISVG for SAP-related functions consists of:

- People or identities
- SAP accounts (SAP Users), permissions (SAP Roles) and relationships
- SAP fine-grained authorization objects, such as transactions, fields and value, and the mapping to SAP Roles
- SAP Authorization Patterns
- Business Activities
- Business Activity to SAP Authorization Pattern mapping
- Risk definitions

Note that the business activity to permission (SAP Role) mapping in ARC will be derived from the business activity to SAP Authorization Pattern mapping in ARCS.

There are different approaches and tools to collect and consume these datasets.

Loading Identities into ISVG

Identities will normally be stored in some form of HR system or some other identity store (perhaps Active Directory is the store). The following mechanisms could be used to load identities into ISVG

- For employees etc. stored in SAP HR, we can use the ISVG SAP Connector to automatically load the identities into ISVG
- For other HR systems, you could build a custom HR Feed mechanism to automatically push identities into ISVG. This has been done with Tivoli Directory Integrator in the past.
- There is a generic CSV-based identity connector in ISVG that could be used to load identities.
- There are bulk load tools available with ISVG to load identities. These would need to be extracted from an identity store somehow and massaged into ISVG's format.

There are other options, but these are the common ones.

Loading SAP Accounts and Permissions

The ISVG SAP Connector will automatically pull the accounts (SAP Users) and permissions (SAP Roles) and relationships into ISVG. The provisioning adapters will do the same.

There are also bulkload tools that can be used.

Loading SAP Fine-grained Authorization Objects

The fine-grained authorization objects must be collected and consumed via the SAP Connector Agent directly into ARCS. There is no other mechanism to load them.

Loading SAP Authorization Patterns

Recall that SAP Authorization Patterns aren't physical objects in SAP or elsewhere, they are logical definitions that someone has to come up with. Where do they come from?

- The local SAP expert – someone who understands the SAP implementation and can identify the granular transaction-based combinations of AO's that are needed to perform a function.
- An audit report – a recent audit may have identified the needed combinations of AOs for a set of transactions
- Our pre-canned definitions – due to recent work with a partner we have a set of Authorization Pattern definitions for Financial (FI**) transactions that can be used. This is a starter set; they may need to be tweaked to suit local AO values (e.g., company codes), work is still required for the other SAP modules, and they will never cover local transactions (z***).

There are two ways to load SAP Authorization Patterns; via the UI or using the bulk load tools. The UI may be appropriate for a small environment but not for a large SAP deployment,

There are bulk load tools for creating (inserting) and deleting (removing) SAP Authorization Patterns, and to "Add a SAP Authorization" to a business activity, and "Remove a SAP Authorization" from a business activity. There are no bulk load tools for SAP Roles, AO's and transactions.

Loading Business Activities

The business activities, and business activity tree, may come from a number of sources:

- A company may already have a set of business activities defined.
- A recent audit may have provided a set of business activities.
- They are using SAP GRC AC and it has a set of business activities defined.
- We provide a standard set of business activities for many of the functions related to SAP modules
- We provide a standard set of business activities from the APQC initiative.

Business activities can be manually entered into ISVG via the UI or bulk load tools are available. There is no OOTB mechanism to pull business activities from SAP GRC AC.

Loading Business Activity to SAP Authorization Pattern Mapping

This data relies on the definition of both business activities and the SAP Authorization Patterns. Thus, the mapping is unlikely to be pre-available anywhere and will need to be built based on expert knowledge or any pre-canned definitions we can supply.

We have a set of business activities, SAP Authorization Patterns and the mapping between them for SAP Financials and this will grow over time to include more data.

The mapping can be performed in the UI or via the bulk load tools. There is a “Add SAP Authorization to Activity” import and a “Remove SAP Authorization from Activity” import.

The data would need to be formatted for the XLS structure used.

Note that there is automatic synchronization from ARCS to ARC that will take the BA <-> SAP Authorization <-> SAP Role relationship and convert it into a BA <-> SAP Role relationship.

Loading Risk Definitions

Risks are combinations of business activities with some other settings (like level). Risk definitions will come from:

- The local SAP expert – someone who understands the SAP implementation and can identify the SoD/SA risks.
- An audit report – a recent audit may have identified the needed combinations of BAs.
- SAP GRC AC – contains risk definitions that could be consumed.
- Our pre-canned definitions from earlier work.

Risks are defined in the ARC module in the UI or via the bulk load tools in ARC (not ARCS). There is no OOTB mechanism to collect risk definitions from SAP GRC AC.

Technical Aspects of the SAP Connectors and Tasks

When talking about the ISVG SAP Connector we’re actually talking about two things; the SAP Connector (JCo-based) that implements the HR Feed and course-grained reconcile/provisioning and the SAP Connector Agent fine-grained governance.

Ignore the terminology, the SAP Connector and SAP Connector Agent are two independent integrations used by different modules in ISVG

ISVG SAP Connector (for AGC and ARC)

The SAP Connector includes server-side definitions and the SAP Java Connector libraries. For working with SAP Users and SAP Roles in AGC/ARC, there is no agent to be deployed. The SAP Connector is agentless, using the JCo calls.

Installing JCo and the SAP Connector

ISVG is pre-loaded with all the server-side components for the SAP Connector, except the Java Connector libraries.

The SAP Java Connector is a standard remote Java-based API provided by SAP. It is used by any vendors needing to remotely connect to SAP. Our (ISIM) Provisioning Adapters use it.

There are two files needed: libsapjco3.so and sapjco3.jar.

The files are packed in a platform specific download that the customer must obtain from SAP for their SAP environment. For ISVG we need the Linux 64-bit files.

These files need to be imported into the ISVG Virtual Appliance. This is done using the Local Management Interface. See [SAP Libraries - IBM Documentation](#)

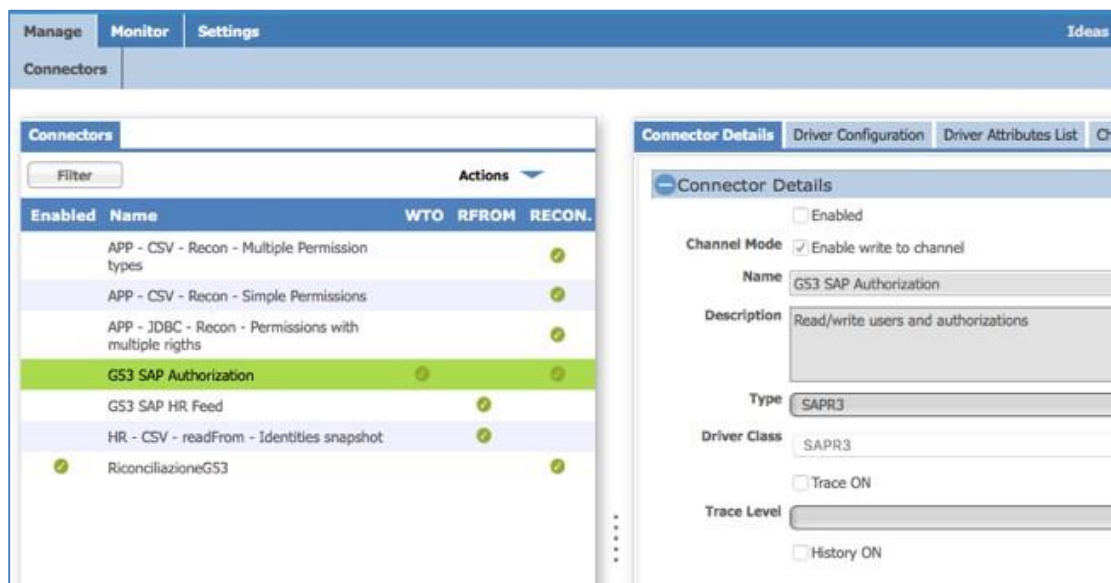
Configuring a SAP Connector in Enterprise Connectors

With the JCo libraries loaded, the SAP Connector can be configured in ISVG. The SAP Connector Agent is only used by the ARCS module and its setup will be discussed later.

Note that an **Application** and **Account** should be defined for the SAP system prior to configuring the connector. The **Events Marker** will be needed in Connector configuration.

The connector is defined in the Enterprise Connectors function within the Admin Console.

When creating the connector, the Type must be “SAPR3” and the Driver Class “SAPR3”.

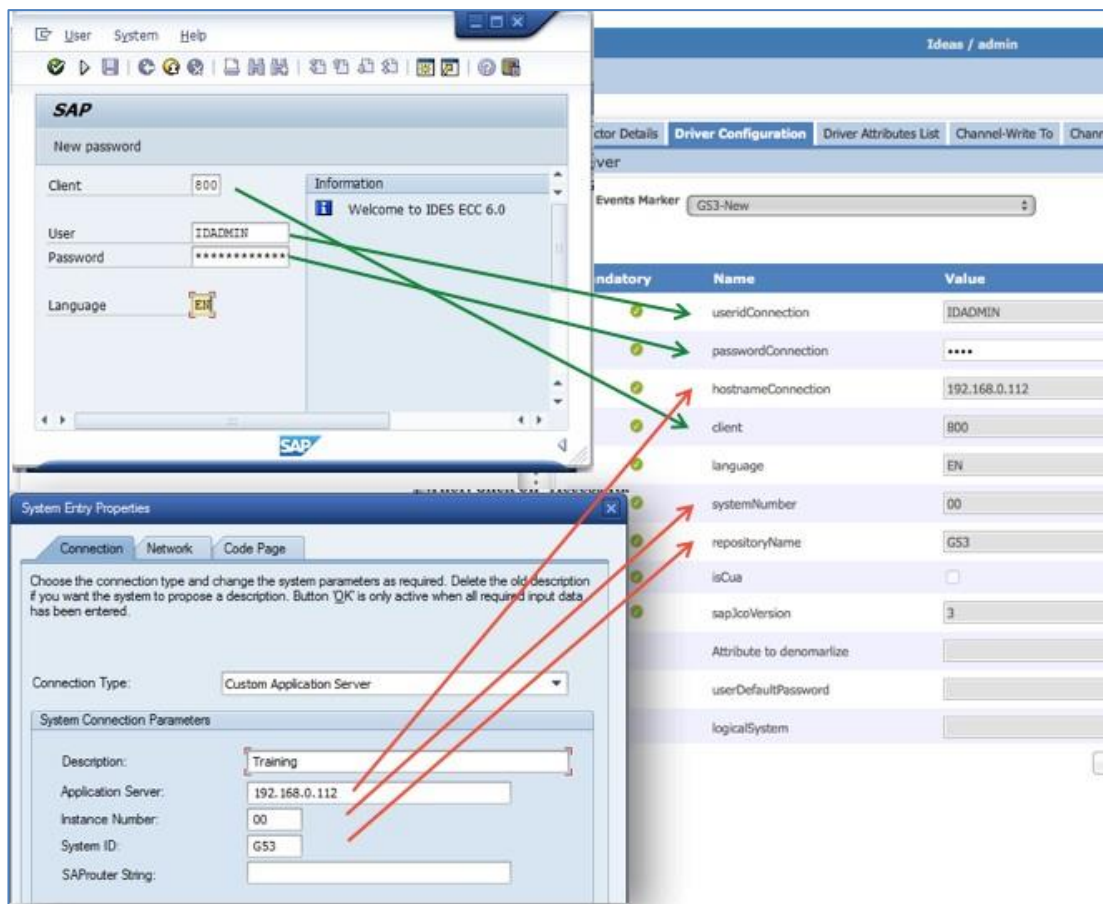


Enabled	Name	WTO	RFROM	RECON.
	APP - CSV - Recon - Multiple Permission types			✓
	APP - CSV - Recon - Simple Permissions			✓
	APP - JDBC - Recon - Permissions with multiple rights			✓
	G53 SAP Authorization	✓		✓
	G53 SAP HR Feed		✓	
	HR - CSV - readFrom - Identities snapshot		✓	
✓	RiconciliazioneG53			✓

Connector Details	
Channel Mode	<input type="checkbox"/> Enabled <input checked="" type="checkbox"/> Enable write to channel
Name	G53 SAP Authorization
Description	Read/write users and authorizations
Type	SAPR3
Driver Class	SAPR3
Trace Level	<input type="checkbox"/> Trace ON <input type="checkbox"/> History ON

Once the connector is created, it can have either of both of the “write to channel” and “reconciliation channel.” The first is for provisioning, the second is for reconciling the users, roles and authorization objects.

The **Driver Configuration** tab is used to specify the connection settings. The following figure shows a sample configuration and how the values are gleaned from SAP.

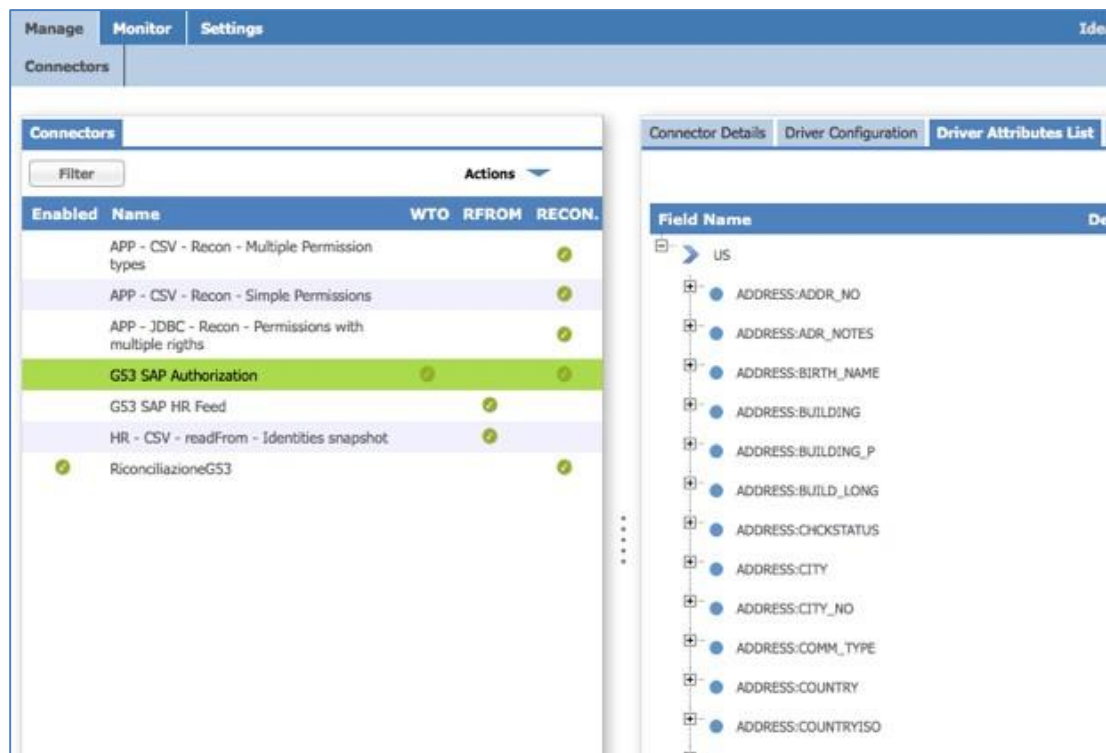


The mandatory fields are:

Field	From
useridConnection	Unique SAP User created for the connection
passwordConnection	Password for unique SAP User created for the connection
hostnameConnection	IP address or hostname for the SAP server being connected to (System Entry Properties)
client	SAP client ID for the connection
language	System language
systemNumber	Instance Number for SAP system (System Entry Properties)
repositoryName	System ID for SAP system (System Entry Properties)
isCua	Whether SAP is using CUA (Central User Administration) or not
sapJcoVersion	The version of the JCo libraries installed (probably 3, but depends on what the customer has downloaded and provided for their SAP installation).

With these settings set, the connection to SAP can be tested.

The Driver Attributes List tab allows definition of the SAP schema. There is an Automatic Add action (Actions menu) that will populate this list from SAP using the connector.



With the SAP attributes known, mapping can be configured for the Channel-Write To (ISVG person to SAP account) and the Channel-Reconciliation (SAP account to ISVG person).

The connector configuration is complete, and a reconcile can be run to load the SAP data into ISVG.

ISVG SAP Connector Agent (for ARCS)

The ARCS module uses a direct connection to SAP and a set of BAPI modules installed there, called the SAP Connector Agent. This connection does not use the SAP Connector.

Installing the SAP Connector Agent

The Connector Agent is a series of BAPI modules that are installed on the SAP system and collect the authorization objects to send to ISVG.

Details on the SAP Connector Agent (aka SAP Adapter Agent), including installation instructions, can be found in the online product documentation:

[Introduction to the ARCS-SAP adapter agent - IBM Documentation](#)

The agent can be downloaded here: [IBM Products](#)

Note that this is not the normal provisioning adapter download mechanism.

The agent consists of five jobs:

z_start_sync	This feature creates a SAP job that makes mass extractions of SAP authorization data and populates the relative data and log tables.
z_get_job_status	This function returns the status and log of the SAP job launched with the z_start_synch command.
z_get_sync_data	This command allows the ARCS module to receive packaged authorization data from the tables in the queue.
z_get_single_role	This function returns the authorization information to ARCS for an individual role, provided as an Input (Import) parameter.
z_get_tcode	This function returns to ARCS the existing transaction codes associated to the Input (Import) data values.

The documentation describes the limited configuration required. This includes creating a new role Z_ARCS_REMOTE.

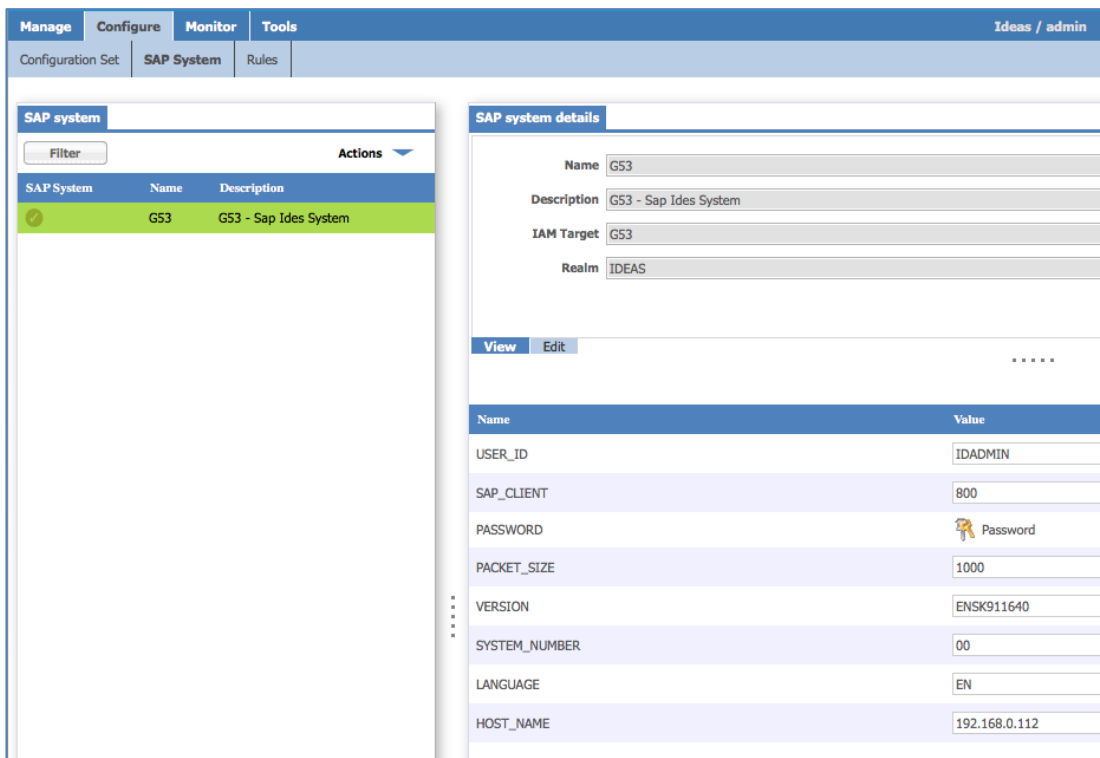
Once the agent is installed, there should be no need for ongoing maintenance other than patching the agent code.

Note that there's currently an issue with the role needed for the agent:


[ARCS-SAP Adapter Agent installation failure \(ibm.com\)](#)

Configuring a SAP Instance in ARCS

Prior to loading the fine-grained authorization objects into the ARCS module, the SAP system must be defined to ARCS. This is equivalent to defining the SAP Connector described earlier.



The screenshot displays the ARCS configuration interface. The top navigation bar includes 'Manage', 'Configure', 'Monitor', and 'Tools'. The current view is 'SAP System' under 'Configuration Set'. A table on the left lists the SAP system 'G53' with the description 'G53 - Sap Ides System'. The right pane shows the 'SAP system details' for 'G53', including the description 'G53 - Sap Ides System', IAM Target 'G53', and Realm 'IDEAS'. Below this, a table lists various configuration parameters and their values:

Name	Value
USER_ID	IDADMIN
SAP_CLIENT	800
PASSWORD	 Password
PACKET_SIZE	1000
VERSION	ENSK911640
SYSTEM_NUMBER	00
LANGUAGE	EN
HOST_NAME	192.168.0.112

The fields are:

Field	From
USER_ID	Unique SAP User created for the connection
SAP_CLIENT	SAP client ID for the connection
PASSWORD	Password for unique SAP User created for the connection
PACKET_SIZE	To control the size of packets flowing
VERSION	This is a value built from the agent and SAP system
SYSTEM_NUMBER	Instance Number for SAP system (System Entry Properties)
LANGUAGE	Language of the SAP system
HOST_NAME	IP address or hostname for the SAP server being connected to (System Entry Properties)

There is an action to Verify the settings. Once the SAP System is defined, there is a Data Refresh Tool to “Load from SAP” that must be run.

Synchronising Fine-Grained (ARCS) to Coarse-Grained (ARC)

Whilst the Access Risk Control for SAP (ARCS) module can operate independently for some analysis and reporting, it works best when integrated with the other ISVG modules – the core (AGC), Access Risk Control (ARC) and the warehouse.

ISVG Users, SAP Users and SAP Roles Between ISVG Modules

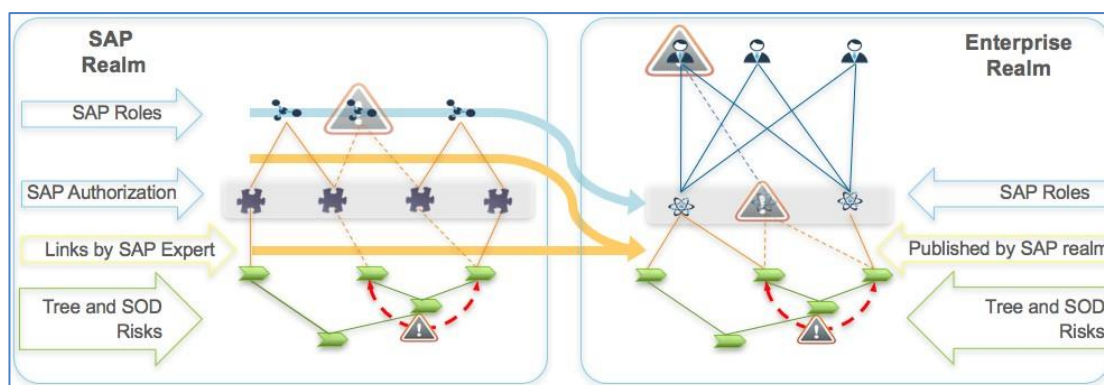
Users (ISVG Users), Accounts (SAP Users), Permissions (SAP Roles) and the relationship between these are stored in the identity warehouse and made available to the different modules, like ARCS. There is no “synchronization” that needs to take place.

Business Activity and Risk Mapping between ARC and ARCS

The risk definition in ARCS has SoD/SA rules containing business activities, business activities mapped to SAP Authorization Patterns, and a correlation between SAP Authorization Patterns and SAP Roles (and users).

The model in ARC is based on SoD/SA rules containing business activities, business activities mapped to SAP Roles (permissions), and SAP Role mapped to users.

These relationships are shown in the following figure.



To take the ARCS definitions and use them to define ARC definitions, the SAP Role <-> SAP Authorization Pattern mapping + SAP Authorization Pattern <-> Business Activity mapping in

ARCS must be translated into a SAP Role <-> Business Activity mapping in ARC. This is shown by the yellow arrows in the figure above (the blue arrows show SAP Roles in ARCS to SAP Roles in ARC).

There is a task that can be run to perform this migration. See for details:

[Business Activity Mapping: ARCS to ARC - IBM Documentation](#)

There is also a task (actually part of the same AccessRiskControls4SAPSync task) to synchronize changes made to the business activity tree in ARC with ARCS. See for details:

[Activity Tree: aligning ARC to ARCS - IBM Documentation](#)

ARCS Data Refresh Tasks

ARCS includes some tasks found under the Tools -> Data Refresh -> Schedule Operations tab in ARCS. They are listed at:

[Data refresh - IBM Documentation](#)

The tasks are:

Load Data from SAP	This task connects to the SAP Connector Agent and collects all the authorization objects and build the Role->Txn+AO mappings
SoD Analysis	This is the main SoD analysis. Needs to be run after the Load.
SAP Role Analysis	This will run through each role and identify the SAP Authorizations that apply.
Collective Role Analysis	This processes the collective roles - Collective roles are association of SAP roles created in SAP.
User Analysis	This is used for a deep SAP analysis. We consider all user's SAP roles as a unique role (cluster) and perform analysis on it (like SAP Role Analysis). Based on SAP authorization definition, we can have a different result if we consider single user's roles analysis and cluster analysis. It's possible cluster analysis to discover association with SAP authorization not discovered during single roles analysis.
Warning Analysis	Runs the best-practices analysis. Warning analysis leverages on Rule Engine capability and customer can define his best practices. The best is run it after load and analysis

After any update related to SAP/Collective Roles or Users, the first operation that you have always to run is the SoD Analysis. After the SoD Analysis, you can choose the operation that you need. A best practice is to run this sequence:

1. SoD Analysis
2. SAP Role Analysis (if you need)
3. Collective Role Analysis (if you need)
4. User Analysis (if you need)

Provisioning with the ISVG SAP Connector

Provisioning SAP accounts (SAP Users) and SAP Role membership changes from ISVG is no different to any other system. After ISVG has processed the changes, they are written to the Out queue, where they are picked up and processed by the SAP Connector and applied to SAP.

The connector will not create SAP Roles, but it will create SAP accounts if the user does not have one and a SAP Role is assigned to them.

Note that there are currently some technical challenges with provisioning using the SAP Connector in some environments. It may mean needing to use the SAP Provisioning Agents.

SAP Provisioning Adapters

In addition to the legacy (from CrossIdeas) SAP Enterprise Connector discussed in the previous sections, ISVG can also use the various Provisioning Adapters that have come from the IBM Security Identity Manager (ISIM) heritage.

The full list of supported provisioning adapters can be found in the ISVG product documentation:

[Identity Brokerage Adapters - IBM Documentation](#)

At the time of writing the following SAP provisioning adapters are supported with ISVG:

- SAP HANA Database
- SAP NetWeaver
- SAP Sybase DB
- SAP UME (Portal)

Each of these adapters have their own deployment and configuration (summarized in the following sections) but will all be configured in the Target Administration UI, run from Identity Brokerage component of ISVG, and present a set of accounts and permissions to ISVG via the Broker-Governance interface (i.e., the ISVG Out and Target queues).

Note that there is also some integration between IBM Security Identity Manager (ISIM) and SAP GRC Access Control. This leverages SAP GRC AC for SoD checks and optionally for provisioning. In its native form it can't be used with ISVG as it involves extending the ISIM workflows for account management, but there has been some services work done to leverage it (discussed in the last section of this document). For more details see

[SAP GRC integration scheme - IBM Documentation](#)

SAP HANA Database Provisioning Adapter

SAP HANA is an in-memory, column-oriented, relational database management system developed and marketed by SAP SE. It is the datastore used by many SAP modules. It can be on-premise or cloud.

The adapter automates these user account management tasks:

- Reconciling user accounts and other support data
- Adding user accounts
- Modifying user account attributes
- Modifying user account passwords
- Suspending, restoring, and deleting user accounts

It does not create/delete supporting data (groups).

The adapter is TDI-based. It needs the SAP HANA JDBC driver (called ngdbc.jar) which is installed in the [TDI_HOME]/jars/3rdparty/others folder.

The adapter requires a SAP HANA admin account with the sap.hana.admin.roles.Administrator privilege. It also needs the SAP HANA Service name and URL.

Further adapter information can be found in the **SAP HANA Database Adapter Installation and Configuration Guide** :

[SAP HANA Database Adapter Installation and Configuration Guide - IBM Documentation](#)

SAP NetWeaver

SAP NetWeaver is the primary technology computing platform of the software company SAP SE, and the technical foundation for many SAP applications. It is a solution stack of SAP's technology products. The SAP Web Application Server (sometimes referred to as WebAS) is the runtime environment for the SAP applications, and all of the mySAP Business Suite solutions (SRM, CRM, SCM, PLM, ERP) run on SAP WebAS.

This adapter is equivalent to the SAP Connector operating in a coarse-grained governance and provisioning mode. It reconciles and provisions SAP Users, SAP Roles (reconcile only) and role memberships.

The adapter automates several administrative and management tasks.

- Creating users and groups
- Modifying users' attributes
- Changing user account passwords
- Suspending, restoring, and deleting user accounts
- Reconciling users and user attributes

In some cases, the standard features and functionality of SAP may not satisfy business requirements. The adapter supports configurable extension and customization for you to map the adapter to your desired requirements. The primary mechanism enabling this is XSL stylesheets, which can be installed with the adapter.

The adapter is TDI-based. The TDI AssemblyLines use the Tivoli Directory Integrator SAP User connector and RFC functional component to enable user management-related tasks on the SAP NetWeaver AS ABAP (via the SAP Java Connector, or JCo).

The JCo libraries must be installed on the TDI server (ISVG VA or remote server running TDI). The JCo libraries are provided by the customer as they need to be obtained from SAP support for the customer's specific SAP environment. There are some constraints on JCo versions and TDI JVMs. See the documentation for details.

The adapter also needs some stylesheets and jars installed.

The adapter uses an administrator account to perform operations remotely by using the login ID and password of a user that has administrator privileges. This administrator account needs a role that has the SAP privileges of: S_RFC, S_RFCACL, S_TABU_DIS, S_USER_GRP, S_USER_AGR, S_USER_PRO, and S_USER_SYS.

The adapter includes a Complex Attribute handler. Whilst it could be enabled in ISVG, there is no way to manage the complex attributes given the current governance-broker mechanism. Also, the ability to adjust the mapping of data using the stylesheets has limited use in the current ISVG.

The SAP NetWeaver adapter supports an extensive list of SAP User attributes (over 40). However, the governance-broker interface currently limits the attributes that can be passed from an ISVG User (person) to a broker target account (e.g., SAP User) to userid, password, firstname, surname, email and org unit. If you need to manage a wider set of attributes, you should look at the SAP (Enterprise) Connector instead of the SAP (Provisioning) Adapter.

Further adapter information can be found in the **Directory Integrator-based Adapter for SAP NetWeaver Adapter Installation and Configuration Guide**:

[Directory Integrator-based Adapter for SAP NetWeaver Adapter Installation and Configuration Guide - IBM Documentation](#)

SAP Sybase DB

Sybase is an acquisition for SAP and not a core SAP product. Details of the adapter can be found at:

[Sybase Adapter Installation and Configuration Guide - IBM Documentation](#)

SAP UME (Portal)

The user management engine (UME) provides a centralized user management for all Java applications and can be configured to work with user management data from multiple data sources. It is seamlessly integrated in the SAP NetWeaver Application Server (AS) Java as its default user store and can be administrated using the administration tools of the AS Java.

The adapter automates administrative tasks on SAP User Management Engine Application Server Java.

- Creating users
- Modifying users' attributes
- Changing user account passwords
- Suspending, restoring, and deleting user accounts
- Reconciling users and user attributes

In some cases, the standard features and functionality of SAP might not satisfy business requirements. The adapter supports configurable extension and customization for you to map the adapter to your desired requirements.

The adapter uses a special TDI SAP User Management Engine Application Server Java connector that ships with the adapter and must be installed into TDI (jar and a properties file).

The adapter uses the SPML (Service Provisioning Markup Language) standard. SAP provides out-of-the-box SPML provisioning link with SAP Application Server Java.

The adapter requires an administrator account on the managed resource that has administrative rights and SPML provisioning rights. For example, you want to manage Resource1 and the SAP User Management Engine Adapter is installed on Resource1, then Admin1 account must have a Role containing the following SAP authorization objects: spmlRole, spml_Write_Action, spml_Read_Action and \$SAP_J2EE_Engine_Upload.

Further adapter information can be found in the **Directory Integrator-based Adapter for SAP User Management Engine Adapter Installation and Configuration Guide**

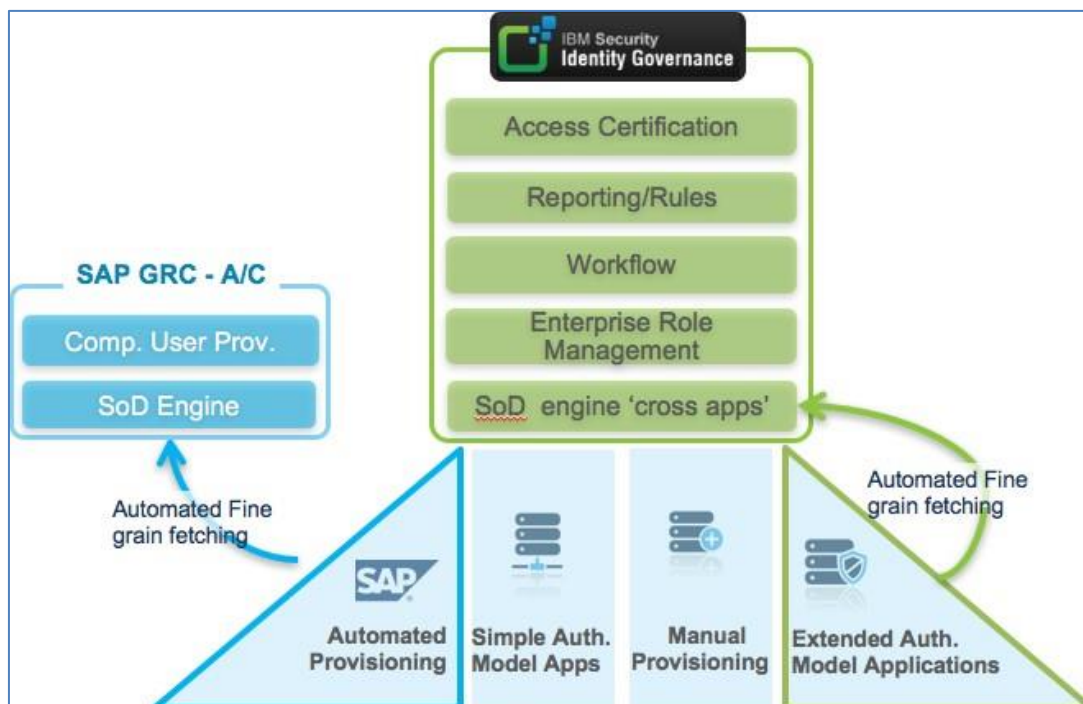
[Directory Integrator-based Adapter for SAP User Management Engine Adapter Installation and Configuration Guide - IBM Documentation](#)

ISVG and the SAP GRC Access Control for SoD Checking

With ISVG 10.0.1 some integration points were introduced to allow custom integration for external SoD engines and calls out to a ticketing system. These can be used to build SAP-related integration, such as:

- Calling SAP GRC AC for a SoD decision, and
- A services-developed integration to leverage SAP GRC AC

The following figure shows the components involved:



ISVG is providing the governance and provisioning functionality (green boxes), including the SoD engine for applications across the enterprise. This includes governance and provisioning for many systems including SAP (blue sections at the bottom) as discussed earlier in this document.

There is also the SAP Governance, Risk and Compliance (GRC) Access Control (AC) module that contains its own SAP-specific SoD engine and Compliant User Provisioning (CUP) which provides, access request self-service, approvals, compliance checks, proactive resolution of access controls, and provisioning. It is an interface used by many provisioning solutions, like ISIM, to provision into SAP and leverage the SoD checks,

Thanks to Marco Venuti for the images and deck I've used to produce this section of the document.

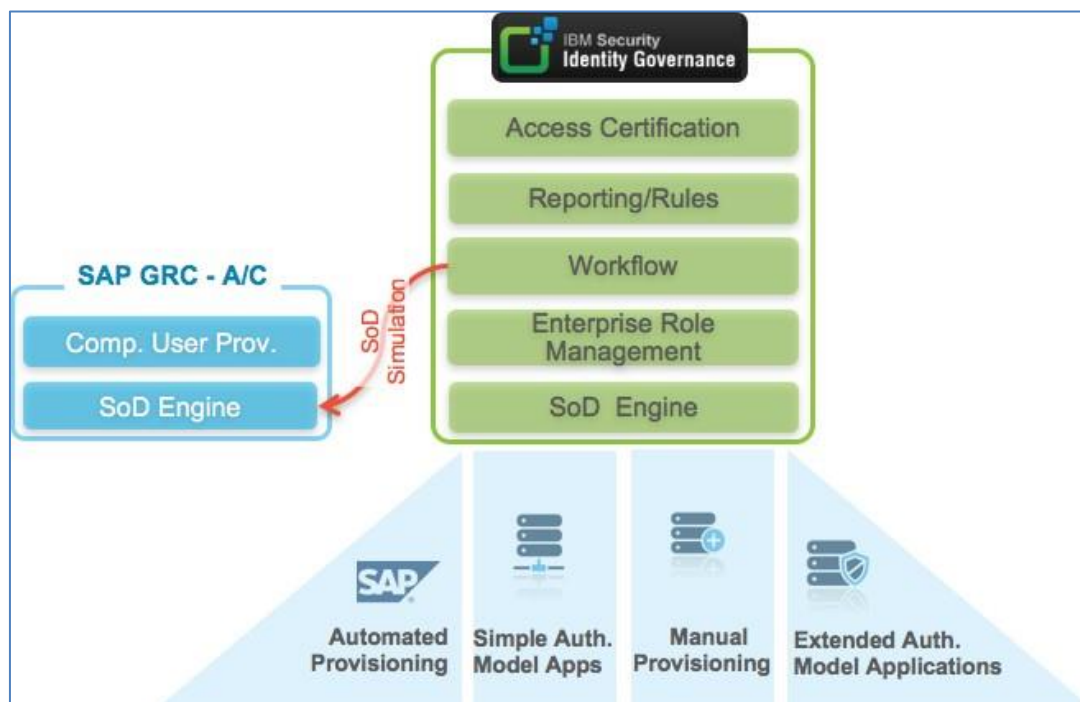
Note that some of the material here is services-based or work-in-progress. The interfaces are there but some configuration/customization work is still required.

Using SAP GRC AC for External SoD Checks

With this integration the external SoD engine, i.e., the one in SAP GRC Access Control, is used instead of the ISVG SoD engine.

Overview of the Integration

The following figure shows the key components and integration.



It involves an ability introduced into the ISVG ARM engine to invoke external SoD engines, such as SAP GRC- AC RAR Module. At the appropriate point in the workflow, ISVG will make a call out to the SoD engine in SAP GRC AC for a SoD check and use the response as if it had been produced by the internal SoD engine.

A sample has been developed for a customer deployment, called the “SAP GRC AC SoD Engine Wrapper for ISVG SoD Simulator.” It provides:

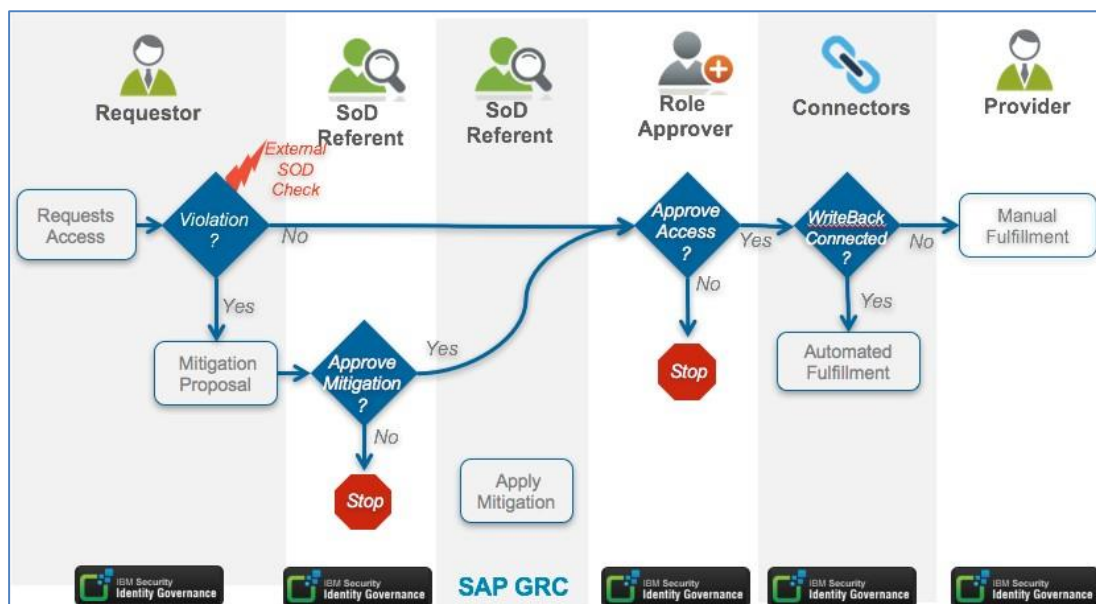
- The ability for ARM to call GRC SoD Simulator API
- The conversion of the result into the native ISVG format, including the extraction of the violation description in terms of conflicting business activity and linked Roles

The integration uses the `cl_grac_sod_risk_analysis` ABAP function via RFC.

It is not shipped as an OOTB product function, it needs to be shared within the technical community and would form the basis for local customization for a specific customer SAP environment.

Sample Flow with External SoD Check

The following diagram shows a sample flow for an access request in ISVG with this integration.



After the user initiates the request, ARM would do its normal SoD/SA check. However, in this case it's making an external call out to SAP GRC AC for the SoD check. The result will flag a violation or not.

If there is a violation, the request will be routed to the risk owner ("SoD Referent") the same as for any other ISVG access request. They can approve the request or reject it. If they reject it, the request will stop.

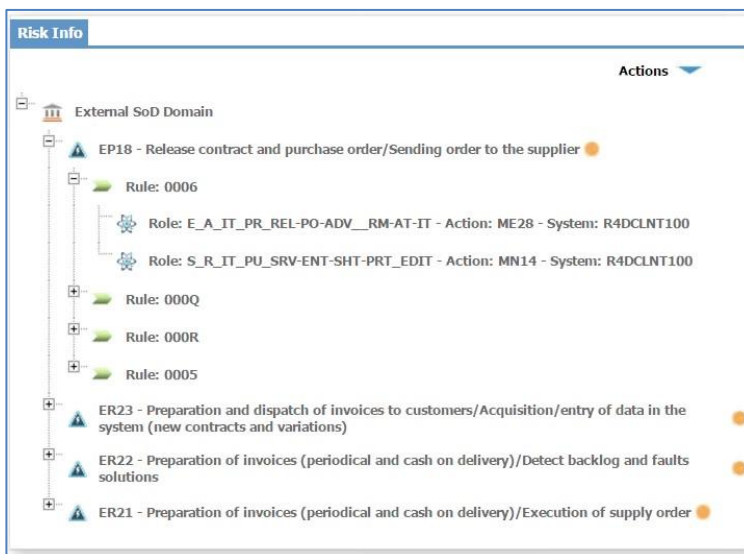
With this flow the mitigation is not applied in ISVG. It is applied in GRC. This is why the diagram shows the two blue lines going across the second SoD Referent box in the diagram. The same person, the risk owner, approves the risk in ISVG and also applies the mitigation in SAP GRC.

From here the flow continues as normal.

Violation Visibility in ISVG

With the SoD checks being performed in SAP GRC, how do we provide visibility into the risks? There needs to be a bulk-load of business activities, risks and mapping from SAP GRC into ISVG.

This will present a very SAP-like view of the risks. An example is shown below.



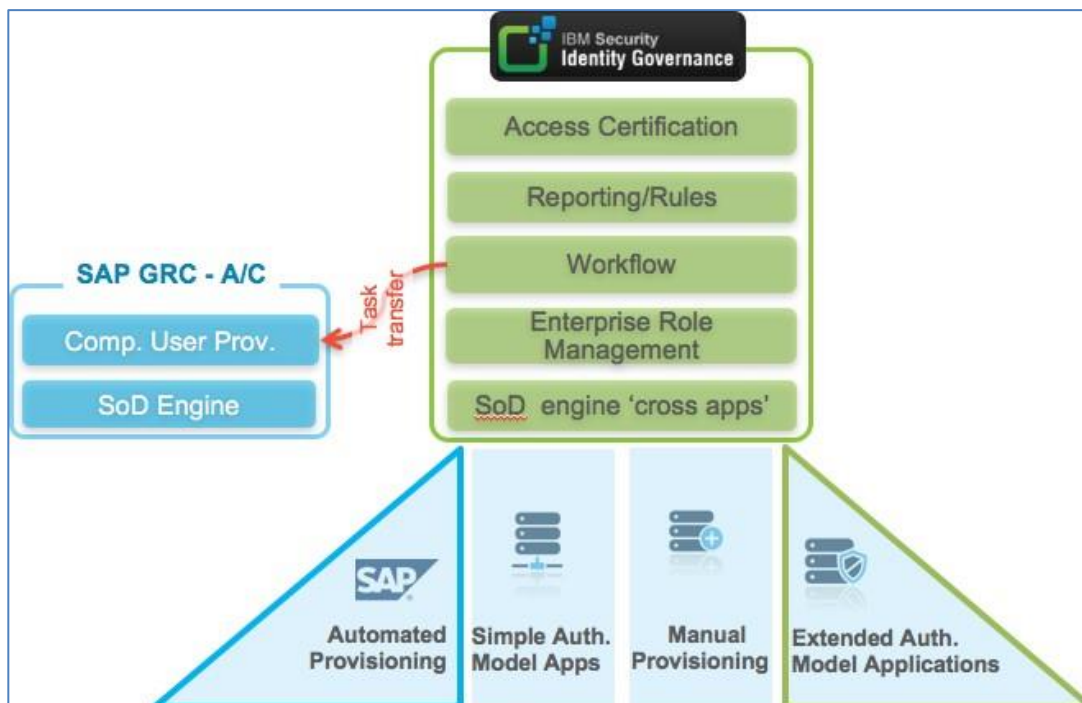
We see the SAP GRC risk definitions (name and description), rules comprising those risks and the permissions to map to them.

Task Transfer – SAP GRC AC as a Step in Workflow

This second approach uses SAP GRC Access Control like a ticketing system called as part of the ISVG access request workflow.

Overview of the Integration

The following figure shows the key components and integration.



In this integration, ISVG is calling the Compliant User Provisioning (CUP) module using its APIs to perform a step in the approval workflow.

It is using a new capability in the ISVG Access Request Module (ARM) to call an external ticketing system and await a response. In this case the external ticketing system is the SAP GRC/CUP module.

The SAP GRC/CUP module adapter for Task Transfer provides:

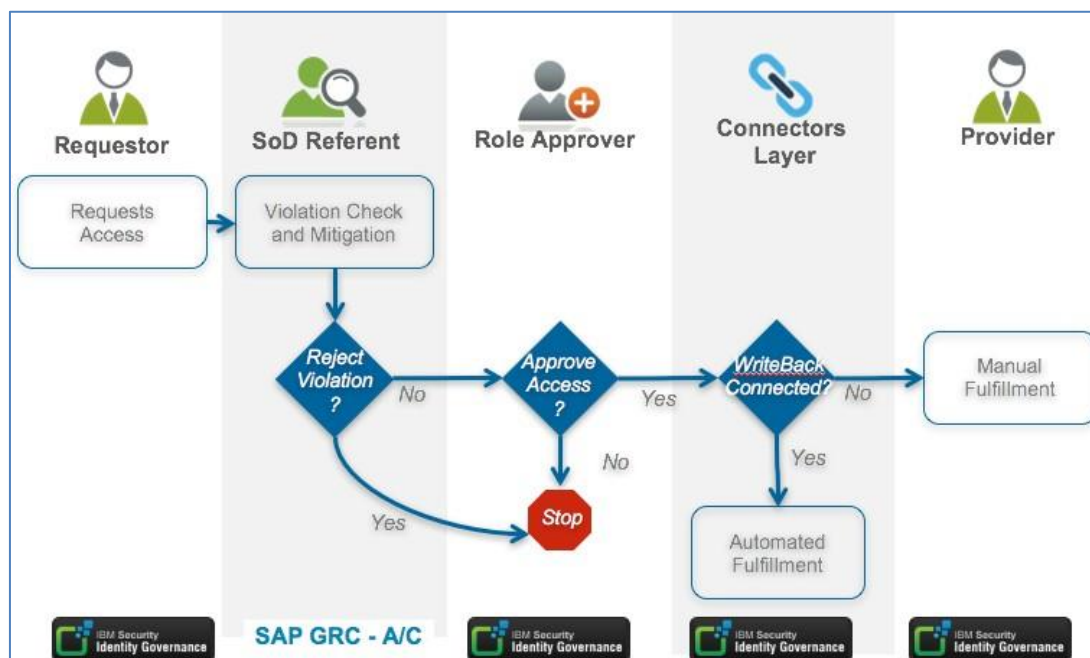
- The ability for ARM to trigger a new workflow item into SAP GRC/CUP
- The ability to poll for the completion of the workflow request including the extraction of the description of the Violation and mitigation control selected in SAP GRC AC, when applicable

The integration approach involves an ISVG initiated - Web Services calls based on well documented SAP GRC Access Control Web service interface. This integration is derived from the existing ISIM GRC integration.

This was developed by professional services as part of a deployment and is currently not OOTB product functionality.

Sample Flow with Task Transfer

The following diagram shows a sample flow for an access request in ISVG with this integration.



The Requestor performs the access request. The Access Request Module immediately hands this off to SAP GRC AC (CUP) as if it was an external ticketing system.

The CUP module provides the violation check and mitigation options for the SoD Referent (via the SAP UI). The final action is to accept or reject the violation in SAP.

If the violation is approved, then the flow returns to ISVG and continues as normal.

Whereas the external SoD check is configured across the board (AGC -> Settings -> General), the ticketing integration is applied on a per-workflow instance and so can be enabled for a subset of workflow scenarios.

Implications of the Task Transfer Approach

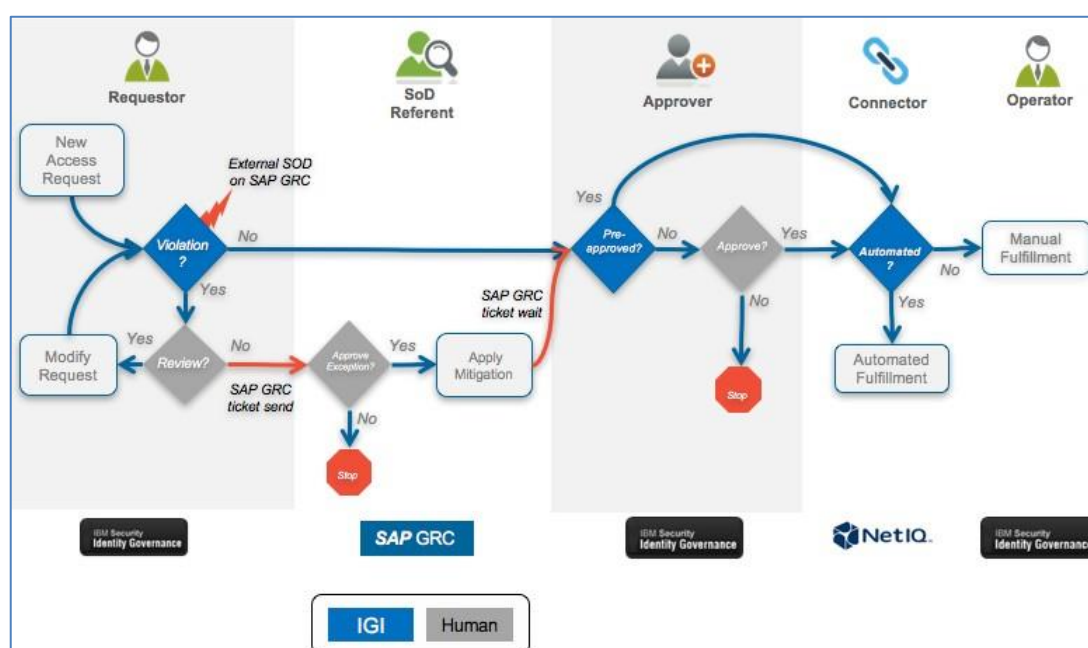
All SoD reviewer / mitigation occurs in SAP GRC AC (CUP). It is an asynchronous SoD check. There will be no visibility of risks/violations/mitigations in ISVG as its being done in SAP.

The workflow involves two UIs, some persona's will use ISVG, and others will use SAP.

The SoD Violation report will need to be generated in SAP, not ISVG.

Combining the Integrations

The two integration approaches can be combined. An example is shown below.



In this example, the External SoD check is used during the Access Request process, so SoD violations show up for the user. If there is a SoD violation, then the Task Transfer mechanism is used to create a ticket in SAP GRC. When the risk is reviewed in SAP, and approved with mitigation, flow returns to ISVG for approval and provisioning.

This combined approach provides the best of both mechanisms, with SoD decisions/mitigation in SAP GRC, but also visibility into risk in ISVG.

This concludes the discussion of ISVG-SAP integration.

End of Document