CUSTOMER

Security Guide

Banking services from SAP® 8.0 (FSAPPL400, FSAPPL450)

Target Audience

- System administrators
- Technology consultants

Document version: 8, published on December 19, 2014

History of Changes

The Security Guide is regularly updated and can be found on SAP Service Marketplace at http://service.sap.com/securityguide.

The following table provides an overview of the most important changes that were made in the latest versions.

Version	Date	Description
1.00	September 5, 2011	Initial version
1.01	June 15, 2012	4.3: Additional information on RFC connections (SAP Notes)
2.00	June 21, 2013	4.6: Example roles for Impairment as part of Financial Accounting for Banks added, Information on Source data Aggregation added4.7: Information on code injection vulnerability in function and class builder added 4.8: Information on tracing of authority groups added
3.00	August 23, 2013	Chapter 5 “Business Partner for Financial Services” added 3.1: Note on NetWeaver version for FSPOT400 added
4.00	February 21, 2014	Chapter 3.1 “Technical System Landscapes” divided into 3.1.1 “Technical System Landscapes using FSAPPL400” and 3.1.2 “Technical System Landscapes using FSAPPL450” Chapter 3.9. “Security-Relevant Logging and Tracing” updated Chapter 7.2 “Regulatory Reporting” added
5.00	July 8, 2014	Chapter 6.4 “Collateral Management” added
6.00	August 22, 2014	Chapter 8 “Data Protection” added
7.00	December 05, 2014	Chapter 3.1.2 (“Technical System Landscape using FSAPPL450”) updated
8.00	December 19, 2014	Chapter 7.3 (“Apps for Transactional Banking”) added

Make sure that you have the latest version of this document before you start the implementation. You can find the latest version on SAP Service Marketplace at http://service.sap.com/securityguide → *Industry Solutions* → *SAP for Banking.*

Contents

1 Introduction

This guide contains security-relevant information for the SAP for Banking solution, including component-specific information for *banking services from SAP 8.0* and scenario-specific information for the business scenarios delivered with SAP for Banking.

This guide does not replace the administration or operation guides that are available for productive operations.

1.1 Target Audience

- Technology consultants
- Security consultants
- System administrators

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereas the Security Guides provide information that is relevant for all life cycle phases.

1.2 Why Is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When you use a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system should not result in the loss of information or processing time. These demands on security apply likewise to *banking services from SAP 8.0*. To assist you in securing *banking services from SAP 8.0*, we provide this Security Guide.

This guide contains security-relevant information for *banking services from SAP 8.0*. Generally the data stored in *banking services from SAP* is personal data that is subject to national data protection laws. In particular, information about transactions made by customers who are also bank employees is distinguished by internal agreements (employee accounts). This data must be protected specifically against unauthorized access by other employees. *banking services from SAP 8.0* provides suitable protection mechanisms. You must also be able to ensure that employees cannot change their own personal business data without authorization.

2 Before You Start

2.1 Fundamental Security Guides

banking services from SAP 8.0 is based on SAP NetWeaver technology. Therefore, the corresponding Security Guides also apply to *banking services from SAP 8.0*. Pay particular attention to the most relevant sections or specific restrictions as indicated in the table below.

Fundamental Security Guides

Scenario, Application or Component Security Guide	Most Relevant Sections or Specific Restrictions
SAP NetWeaver Security Guide	
SAP Exchange Infrastructure (XI) Security Guides	
SAP Business Information Warehouse Security Guides	

For a complete list of the available SAP Security Guides, see SAP Service Marketplace at http://service.sap.com/securityguide.

2.2 Additional Information

For more information about specific topics, see the quick links as shown in the table below.

Content	Quick Link to SAP Service Marketplace or SDN
Security	http://sdn.sap.com/irj/sdn/security
Security Guides	http://service.sap.com/securityguide
Related SAP Notes	http://service.sap.com/notes http://service.sap.com/securitynotes
Released platforms	http://service.sap.com/pam
Network security	http://service.sap.com/securityguide
SAP Solution Manager	http://service.sap.com/solutionmanager
SAP NetWeaver	http://sdn.sap.com/irj/sdn/netweaver
Component Installation Guide and Component Upgrade Guide for *banking services from SAP*	http://service.sap.com/instguides → *Industry Solutions* → *Industry Solution Guides* → *SAP for Banking* → *Component Guides*
Master Guide for Banking with information about banking business scenarios	http://service.sap.com/instguides → *Industry Solutions* → *Industry Solution Guides* → *SAP for Banking* → *Solution Guides*

3 *banking services from SAP*

3.1 Technical System Landscapes

Most SAP for Banking scenarios use component FSAPPL as a business process platform for banking. *banking services from SAP 8.0* is a SAP NetWeaver Add-On that uses functions from the components FINBASIS and SEM-BW.

3.1.1 Technical System Landscapes using FSAPPL400

A minimal system landscape consists of the following components:

- *SAP NetWeaver 7.1 AS ABAP enhancement package 1 for banking services from SAP 7.0* (also valid for *banking services from SAP 8.0)* with the following components:
  - SAP_BASIS
  - SAP_ABA
  - SAP_BW
  - PI_BASIS
  - ST-PI

  Note that while Process Object Types (software component FSPOT400) run on NetWeaver 7.40 on a separate instance, FSAPPL400 cannot be installed on NW 7.40.
- FINBASIS 700
- SEM-BW 700
- BI_CONT (only relevant if you use SAP Bank Analyzer)
- FSAPPL 400

For more information about the technical system landscape, see the resources listed in the table below.

Topic	Guide/Tool	Quick Link to SAP Service Marketplace or SDN
Technical description for *banking services from SAP* and the underlying components such as SAP NetWeaver	*Master Guide*	http://service.sap.com/instguides
High availability	*High Availability for SAP Solutions*	http://sdn.sap.com/irj/sdn/ha
Technical landscape design	See applicable documents	http://sdn.sap.com/irj/sdn/landscapedesign
Security	See applicable documents	http://sdn.sap.com/irj/sdn/security

3.1.2 Technical System Landscape using FSAPPL450

Accounting for Financial Instruments (based on SAP HANA®) as part of banking services from SAP 8.0 (FSAPPL450) is an extension of Accounting and has to be installed on a separate instance. It is based on NetWeaver 7.40 SP5 or higher and can only be used with an SAP HANA database. You can upgrade to FSAPPL450 from FSAPPL400 (SAP HANA enablement only for products Accounting and Financial Database; all other Banking products are not released in FSAPPL450).

A minimal system landscape for FSAPPL450 SP04 consists of the following components:

- *SAP NetWeaver 7.4 AS ABAP* with the following components:
  - SAP_BASIS 740 SP09
  - SAP_ABA 740 SP09
  - SAP_BW 740 SP09
  - PI_BASIS 740 SP09
  - ST-PI 2008_1_710 SP09
- FINBASIS 747 SP04
- SEM-BW 747 SP04
- BI_CONT 747 SP06
- FSCM_CCD 617 SP04
- MDG_FND 747 SP06
- SAP_BS_FND 747 SP06
- WEBCUIF 747 SP06

3.2 User Administration and Authentication

This section provides an overview of the following aspects of user administration and authentication:

- Tools recommended for user administration
- User types required for *banking services from SAP*
- Standard users supplied with *banking services from SAP*
- Integration options in single sign-on environments

banking services from SAP 8.0 uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular SAP Web Application Server ABAP (SAP Web AS ABAP). Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Application Server ABAP Security Guide also apply to *banking services from SAP 8.0*.

3.2.1 User Management

User management in *banking services from SAP 8.0* uses the mechanisms provided with *SAP Web AS ABAP*, for example, tools, user types, and password policies.

User Administration Tools

The table below shows the tools for user management and user administration available with *banking services from SAP 8.0*.

User Management Tools

Tool	Detailed Description	Prerequisites
User and role maintenance for SAP Web AS ABAP (transactions SU01 and PFCG)	For more information, see Users and Roles (BC-SEC-USR)	

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively have to change their passwords on a regular basis, but not those users under which background processing jobs run.

The user types that are required for *banking services from SAP 8.0* include:

- Individual users:
  - Dialog users are used to enter master data and start reports and transactions.
- Technical users:
  - Service users are used for XI communication.

Standard Users

No further users are named in addition to the standard users described in the *SAP Web AS ABAP Security Guide*. All users are created by the customer's system administration, which also provides the initial identification parameters (such as passwords).

3.2.2 User Data Synchronization

banking services from SAP 8.0 does not share any user information with other sources. SAP User Management is private and confidential.

3.2.3 Integration into Single Sign-On Environments

banking services from SAP 8.0 supports the single sign-on (SSO) mechanisms provided by SAP Web AS ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP Web Application Server Security Guide also apply to *banking services from SAP 8.0*.

The supported mechanisms are listed below.

Secure Network Communications (SNC)

SNC is available for user authentication and provides an SSO environment when you use SAP GUI for Windows or Remote Function Calls.

For more information, see *Secure Network Communications (SNC)* in the SAP Web AS ABAP Security Guide.

SAP Logon Tickets

When you use a Web browser as a front-end client, *banking services from SAP 8.0* supports the use of logon tickets for SSO. In this case, users are issued with a logon ticket after they have been authenticated in the original SAP system. The ticket can then be used in other systems (SAP or external systems) as an authentication token. The user does not need to enter a user ID or password for authentication but can access the system directly after the logon ticket has been checked.

For more information, see *SAP Logon Tickets* in the SAP Web AS ABAP Security Guide.

Client Certificates

As an alternative to user authentication with a user ID and password, users with a Web browser as a front-end client can also provide an X.509 client certificate for authentication. In this case, users are identified on the Web server using the Secure Sockets Layer (SSL) protocol and no passwords are required. Users are authorized in accordance with the authorization concept in the SAP system.

For more information, see *Client Certificates* in the SAP Web AS ABAP Security Guide.

3.3 Authorizations

banking services from SAP 8.0 uses the authorization concept provided by SAP NetWeaver AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to *banking services from SAP 8.0*.

The SAP NetWeaver authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the Profile Generator (transaction PFCG) in AS ABAP.

Standard Roles

banking services from SAP 8.0 contains roles that are given as examples and must be adapted. Do not use them in your production system in the form in which they are delivered.

You can display the available roles in the system in Profile Generator (transaction PFCG). The following naming conventions apply:

- Business Partner for Financial Services: SAP_FS_BP*
- Operational scenarios: SAP_FS_CMS*; no template roles are delivered for operational banking
- Analytical scenarios: SAP_BA1*

You can use Profile Generator to create additional roles.

Standard Authorization Objects

banking services from SAP 8.0 uses several authorization objects. You can display the authorization objects in the system in transaction SU21.

The following authorization object classes are used:

- CMSA (Collateral Management System)
- FICO (Financial Services - Financial Conditions)
- FPCO (Financial Services - Posting Control Office)
- FSAM (Financial Services - Account Management)
- FSBA (Financial Services - Bank Analyzer)

- FSDH (Financial Services - Posting Lock Management)
- FSMD (Financial Services - Market Data in Bank Analyzer)
- FSPI (Financial Services - Pricing)
- FSPR (Financial Services - Product Configurator)
- FSTO (Financial Services - Tools)
- PDM (Financial Services - Payment Distribution and Payment Monitoring)
- PPO1 (Postprocessing Office)
- PAM (Payment Advice Management)

Note that the use of authorization objects depends on what functions you use.

The table below shows the security-relevant authorization objects that are used by *banking services from SAP 8.0*:

Standard Authorization Objects

Authorization Object	Field	Value	Description
F_CARD_UML	ACTVT	03	Security Settings for Card Number (Display Accesses)
F_CARD_UMN	ACTVT	03	Security Settings for Card Numbers (Number Display)

3.4 Network and Communication Security

This section provides an overview of the communication paths used by *banking services from SAP* as well as the security mechanisms to be used. It also includes our recommendations for the network topology, so that you can restrict access at network level.

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the back-end system’s database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for *banking services from SAP* is based on the topology used by the SAP NetWeaver platform.

3.4.1 Communication Channel Security

The table below shows the communication channels used by *banking services from SAP*, the protocol used for the connection, and the type of data transferred.

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection

Front-end client with SAP GUI for Windows (workshop interface) to application server	DIAG	All application data	Passwords, personal data
Application server to application server	RFC	All application data	Personal data (for example, account flows, account balances)
Application server to external application	RFC	All application data	Personal data (for example, account flows, account balances)
Application server to application server	HTTP	All application data	Personal data (for example, account flows, account balances)
Application server to third-party application	HTTP	All application data	Personal data (for example, account flows, account balances)

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol. SOAP connections are protected with Web services security.

We strongly recommend using secure protocols (SSL, SNC) whenever possible.

3.4.2 Network Security

Since *banking services from SAP 8.0* is based on SAP NetWeaver technology, for more information about network security see the SAP NetWeaver Security Guide at http://help.sap.com/netweaver.

If you offer services on the Internet, you need to protect your network infrastructure with at least a firewall. You can increase the security of your system (or group of systems) by creating the groups in different network segments, each of which is protected from unauthorized access by a firewall. Remember that unauthorized access can also come from inside if an intruder has already taken control of one of your systems.

Ports

banking services from SAP 8.0 runs on SAP NetWeaver and uses the ports from AS ABAP or AS Java. For more information, see the topics for *AS ABAP Ports* and *AS Java Ports* in the corresponding SAP NetWeaver Security Guides.

3.4.3 Communication Destinations

No RFC destinations are supplied with *banking services from SAP 8.0*. When you set up your non-local data flows, use transaction SM59 to create your RFC destinations. You can copy the role SAP_RFC_CORR_REQ and assign this to the technical writer. For more information, see the documentation for transaction SM59 and the SAP Notes in the SAP Web AS ABAP Security Guide.

User authorizations can become a security risk if used in an irresponsible way. Note the following security rules for communication between two systems:

- Use the user categories *System* and *Communication.*
- Provide users with the minimum authorizations only.
- Choose a secure password and do not reveal this to anyone.
- Save user-specific logon data only for users in the *System* and *Communications* categories.
- If possible, use trusted system functions instead of saving user-specific logon data.

3.5 Data Storage Security

This section provides an overview of all the critical data used by *banking services from SAP* 8.0 as well as the security mechanisms to be used.

The data in *banking services from SAP 8.0* is saved in the system database. There are no special features with regard to the SAP Web AS ABAP Security Guide.

There are no additional locations where data is saved temporarily. A differentiation is made between Customizing data and application data.

- Customizing data is created, changed, and deleted (in certain circumstances) during implementation and partially when the system is live.
- Application data – master data and flow data – is saved in the system during operation.

There are no default settings in the software that specifically protect Customizing data and application data. You need to ensure the level of protection required through suitable assignment of authorizations and system settings (such as client changeability).

Comment:

As described in SAP Note 1434284 (FAQ Authorization concept for generic table access), we recommend you use authorization object S_TABU_NAM in roles if you need to access database tables via transactions SM30/34/SE11/SE12/SE16 because the authorization group is not maintained for all database tables and therefore a check via authorization object S_TABU_DIS is not always sufficiently secure.

Using Logical Path and File Names to Protect Access to the File System

banking services from SAP 8.0 saves data in files in the file system. Therefore, it is important to provide explicit access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following lists show the logical file names and paths used by *banking services from SAP 8.0* and for which programs these file names and paths apply:

Logical File Names Used in *banking services from SAP*

The following logical file names have been created in order to enable the validation of physical file names:

1. BCA_CARD_ORDERFILE_FILE
    - Programs using this logical file name and parameters used in this context:
        - RBCA_CARD_ORDER_ATTR_BCA_CA04
2. BCA_CARD_TEST_FILE

- Programs using this logical file name and parameters used in this context:
  - CARD_CONSISTENCY_CHECK
  - CARD_TRANSFER_FILE

3. BCA_CARD_ORDER_TEST_FILE
   - Programs using this logical file name and parameters used in this context:
     - CCPP_CONSISTENCY_CHECK

Logical Path Names Used in *banking services from SAP*

The logical file names listed above use the logical file paths BCA_AM_CONSISTENT_PATH and BCA_CARD_ORDERFILE_PATH.

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions FILE (client-independent) and SF01 (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log.

3.5.1 Example: Data Storage Security

Using Logical Path and File Names to Protect Access to the File System

The SAP Financial General Ledger Accounting application saves data in files in the file system. Therefore, it is important to provide explicit access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following lists show the logical file names and paths used by General Ledger Accounting and for which programs these file names and paths apply:

Logical File Names Used in This Application

The following logical file names have been created in order to enable the validation of physical file names:

- FI_COPY_COMPANY_CODE_DATA_FOR_GENERAL_LEDGER_0X
  - Programs using this logical file name and parameters used in this context:
    - RFBISA00
    1. RFBISA01
    2. RFBISA51
  1. Parameters used in this context:
     - <PARAM_1> Program name

1. FI_INFOSYS_TRANSPORT
   - Programs using this logical file name:
     - RGRJTE00

1. RGRLTE00
2. RGRMTE00
3. RGRRTE00
4. RGRSTE00
5. RGRVTE00
6. RGRXTE00
7. RGSSTE00
8. RGSVTE00
9. RGRJTI00
10. RGRMTI00
11. RGSSTI00
12. RGSVTI00

1. Parameters used in this context:
   - <PARAM_1> Program name

Logical File Paths Used in this Application

The logical file names listed above all use the logical file path FI_ROOT.

3.6 Security for Additional Applications

If you also use SAP applications that are not explicitly mentioned in this document, their individual security guides apply. These must be considered in an overall security concept.

3.7 Enterprise Services Security

The following sections in the Security Guide SAP NetWeaver 7.0 are relevant for all enterprise services delivered with *banking services from SAP 8.0*:

- *User Administration and Authentication*
- *Network and Communication Security*
- *Security Guides for SAP NetWeaver According to Usage Types -> Security Guide for Usage Type PI*
- *Security Guides for Connectivity and Interoperability Technologies -> Web Services Security*
- *Security Guides for Connectivity and Interoperability Technologies -> Security Guide Communication Interfaces*
- *Security Guides for Operating System and Database Platforms*
- *Security Aspects for System Management*
- *Security Guides for Connectivity and Interoperability Technologies -> Enabling Application-to-Application Processes: Security Aspects*
- *Security Guides for Connectivity and Interoperability Technologies -> Enabling Business-to-Business Processes: Security Aspects*

Accessing Integration Engine Monitoring (transaction SXMB_MONI), for example, requires the NetWeaver role SAP_XI_MONITOR.

3.8 Payment Card Industry (PCI) Security

banking services from SAP 8.0 provides card management functions for its customers. Credit, debit, and other types of cards can be managed within the accounts management contract framework. Credit card payments will not be performed.

Credit card information is displayed within the maintenance transaction of our card management. The display of the credit card information depends on the Customizing settings for the credit card product: It is either masked or in clear text.

3.8.1 High-Level Credit Card Usage

Card management provides administrative functions for all cards. Each unmasked display of the card number will be logged. Tokens are not supported. In the case of credit card fraud, you can inspect the log for the unmasked display of cards to clarify the cause of the fraud.

3.8.2 Implementation

Prerequisites

The encryption is based on SSF technology (Secure Store and Forward). The key is created by Trust Manager. Trust Manager performs the PSE and certificate maintenance functions. For example:

- The creation of key pairs
- The creation of certification requests that have to be signed by a certification authority (CA)
- The maintenance of the list with familiar certification authorities, which the server will accept

To use Trust Manager to create SSL or SNC in Price Calculator Environment (PCE), you must install the SAP Cryptographic Library (SAPCRYPTOLIB).

Customizing

You can assign a card product to the security level in the Customizing activity *Assign Security Level to Card Product*.

The following security levels are possible:

- Unmasked display
- Masked display, but unencrypted save
- Masked display and encrypted save

Furthermore, you can customize the unmasked digits at the start and end of the card number. Up to a maximum of six unmasked characters are possible at the start of the card number and up to a maximum of four characters at the end.

Rotating or Changing Encryption Keys

banking services from SAP 8.0 provides transaction BCA_CARD_SECK for changing the encryption keys. You can use the corresponding report RBCA_CASECK_RUN_PP to rotate the encryption keys periodically when it is included in the bank's end-of-day-processing. The report is assigned to authorization group FA_KEYXG. The transaction and the report do not support the encryption change of archived cards. If you also want to decrypt archived cards

when you create a new key version, the key version valid at time of encryption must still be available. Therefore, we recommend you do not delete the key version before the archiving guidelines allow. Furthermore, we recommend you exchange the keys at least once every six months.

Before you rotate an encryption key you must run the report *Set Global Hash Indicator* (RBCA_CASEC1_RUN_PP) once. Furthermore, in the transaction *Manage Key Versions* you must create a new key version in addition to the current key version. Before it runs the key exchanges the system should end all card processing.

You can delete an encryption key at least 90 days after the key has been exchanged. You can use transaction RSSFV_ADMIN to manage key versions. You can use the transaction to delete old key versions as well. A new SSF application has been created for *banking services from SAP 8.0*: FSCARD. Authorization SSFVADM is needed to execute the transaction.

Masked/ Unmasked Display

Credit card data is shown only for administrative processes within *banking services from SAP 8.0*. The masking can be activated for a card product. This depends on the Customizing settings of the bank and has to be activated if required for a card product. If masking and encryption is activated, the card number is stored automatically in an encrypted and masked form. No further user action is needed to enforce masking.

To display the credit card number in unmasked form, you need authorization F_CARD_UMN.

Logging of Payment Card Number Access

You can use report RBCA_CARD_DISP_LOG to display the log entries for the unmasked display of credit card numbers.

Prerequisites:

- You have the authorization for authorization group FA_KEYLG.
- You have authorization F_CARD_UMN.

Encryption/Decryption and Storage of the Encrypted Number

The credit card number is stored encrypted in the component-specific database BCA_CARD_HEADER.

Migration

The credit card information uses the standard migration functions of card management when you migrate from an old system to a new one.

To activate the encryption function in an already running system, start reports RBCA_CASEC1_RUN_PP and RBCA_CASEC2_RUN_PP.

3.8.3 Deletion of Credit Card Storage

It is not possible to delete stored credit cards without using the archiving function.

3.8.4 Archiving

The credit card information uses the standard archiving functions of card management.

3.9 Security-Relevant Logging and Tracing

This section provides an overview of the trace and log files that contain security-relevant data. If there is a security violation, you can use these to reproduce activities, for example.

Security Incidents like successful or unsuccessful login, changes on user privileges, and so on, are logged using the SAP Web Application Server functionality (Security Audit Log). Detailed information concerning the Security Audit Log is provided in the SAP NetWeaver Application Server ABAP Security Guide.

In order to have the possibility to trace configuration changes the attribute *Log Data Changes* is marked for all customizing tables. The logging can be activated by setting the system profile parameter *rec/client*. The log can be displayed by the transaction *Table History* (SCU3). For additional information consult the SAP NetWeaver Application Server ABAP Security Guide.

All changes to the master data in *banking services from SAP* are registered in the relevant database tables and can be evaluated using change documents.
You can recall the change documents in the relevant transactions by choosing *Display Change Document.*

4 Bank Analyzer

This section contains detailed information about scenarios that use SAP Bank Analyzer within *banking services from SAP 8.0*.

A separate Reporting BI system is used for Bank Analyzer reporting. Therefore, see also the SAP NetWeaver Business Intelligence (BI) Security Guides.

A separate third-party system is needed for the ALM scenario. If you use the ALM scenario, see the documentation for the third-party system.

A general ledger system, such as SAP Business Suite 7.0, is needed for the accounting scenarios of SAP Bank Analyzer. If you use the accounting scenarios, see the documentation for the general ledger system.

4.1 Categorization of Security Risks in Bank Analyzer

The data in Bank Analyzer is used to generate financial statements and disclosure reports that are Basel II compliant. It can also provide the input data for other regulatory reporting interfaces. This means that the data in Bank Analyzer represents some of the information that financial institutions are required to disclose.

Furthermore, the results generated by the analyses in Bank Analyzer are used internally by financial institutions as the basis for managing their business processes and the organization as a whole. So, this data is also of strategic value. The results can also be used to measure the performance of departments and employees.

Some of the data stored in Bank Analyzer is person-related data that is covered by data protection legislation. Information about transactions involving customers who are also employees of the bank (employee accounts) receives special treatment under the banks' own internal procedures.

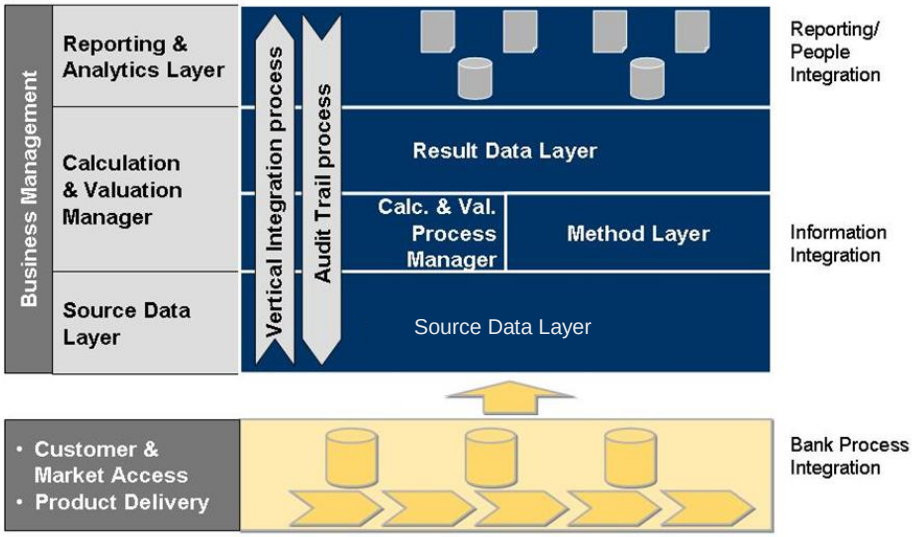
Based on the nature and purpose of the data involved, the security risks for Bank Analyzer can be categorized as follows:

- **Confidentiality/authorization**
  Unauthorized access to data related to persons, which implies the circumvention of data protection legislation, and unauthorized access to data that is of strategic importance, are to be avoided.
- **Integrity**
  Unauthorized data manipulation with the aim of falsifying results is to be avoided.

Bank Analyzer analyzes data that is replicated from operational feeder systems (SAP and non-SAP systems) or that is provided by external organizations (such as market data providers). This document does not cover the security of systems supplying data or the data delivery process, nor does it describe any security measures for avoiding the accidental loss of data or for reducing the impact of data loss, such as the establishment of suitable data backup processes.

4.2 Architecture of Bank Analyzer

This section examines a typical process from start to finish as a way of describing the architecture.



Firstly, input data from various source systems (SAP systems or non-SAP systems, referred to as Customer & Market Access and Product Delivery in the figure above, Analytical Banking: Solution Architecture) is imported into the Source Data Layer using BAPI and service interfaces. The Source Data Layer (SDL) corresponds to the Financial Database (FDB) in previous Bank Analyzer releases.

Before the database is filled, the data has to be converted to the standard data model used in Bank Analyzer. Though SAP NetWeaver BI technology can be used to do this, in technical terms BAPI and service interfaces are always used to load data into the SDL. The SDL stores input information. It also contains business methods, such as those used to generate cash flows from financial conditions and functions for correcting data. It is also possible to write data analyzed by source systems directly in the Results Data Layer (RDL).

The input data taken from source systems is computed and analyzed by the methods and processes in Bank Analyzer. Bank Analyzer's communications framework (data source concept) reads input data and results from upstream methods and processes. The results are stored centrally in the RDL. The central storage of results in integrated structures that can be used throughout Bank Analyzer is new in Release 5.0. In earlier releases, results were stored separately for each Analyzer.

Other methods and processes can be used to compute data for particular information requirements. These methods and processes mainly use the data stored in the RDL but can also access data in the SDL. In this case, the results generated cannot be used for other purposes and are saved locally in the Analytics Layer.

In summary, data is stored in three logical places in Bank Analyzer: general information is stored centrally in the SDL and RDL; specific information is stored locally in the Analytics Layer.

Bank Analyzer Core

The process steps described above calculate and analyze the input data stored in the SDL, and so *produce* results. This part of the solution, including the Analytics Layer, is referred to as the **Bank Analyzer Core** below.

Results are analyzed in SAP NetWeaver BI, not in Bank Analyzer Core. This part of the solution is referred to below as Reporting BI. Reporting BI is a separate system. Bank Analyzer contains DataSources, which replicate data into the Reporting BI system, where it can be used for reporting and analysis purposes.

Bank Analyzer Core is based on SAP NetWeaver and uses the functions of SAP NetWeaver BI. In this context the term Tool BI is used. Although you can use Tool BI remotely, we do not recommend this. If you use SAP NetWeaver BI just as the Tool BI**,** you can apply more restrictive security measures than those described in the SAP Business Information Warehouse Security Guides.

Authorization Objects Relevant for Tool BI

The following roles are relevant for the use of Tool BI:

- If only the user must use the functions of an application, he or she needs the BI authorizations contained in **example role SAP_BA1_SHOW_FDB**.
- If the user must configure the SDL, he or she needs the authorizations of **example role SAP_BA1_EXPERT_BW** for configuring objects in Bank Analyzer that refer to objects in the Tool BI.
- If the user must display all objects of Tool BI that belong to the configuration of the SDL, he or she needs the authorizations of **example role SAP_BA1_SHOW_BW**.

4.3 Network Security and Communication

The network infrastructure is critical for the security of the system. While Bank Analyzer does not have its own communication channels, it uses those described in the SAP NetWeaver Security Guides.

The aspects and measures described in the SAP NetWeaver 7.10 Security Guides (such as the use of SAProuter in combination with a firewall, use of Secure Network Communication (SNC), Communication Front-End Application Server, and connection to the database) also apply for Bank Analyzer.

Internal Data Flows

Internal data flows are those whose source and destination are in the same Bank Analyzer.

Internal data flows can be divided into local data flows, which appear within one logical system, and non-local data flows, which cross the boundaries of a logical system. A logical system is defined as one client in one system.

1. Local data flows in one logical system.

   Function module calls and method calls are used for communication within one client in Bank Analyzer.

   No special security measures beyond those described in the SAP NetWeaver 7.10 Security Guides are required with regard to the security of these internal local calls.

2. Non-local data flows across logical system boundaries

   This type of data flow, which is still within Bank Analyzer but across logical system boundaries, applies to BI systems only (Tool BI or Reporting BI). This type of communication is brought about by Remote Function Call (RFC) or in the data replication process by means of DataSources and IDocs. This type of communication

is secured by SAP's Secure Network Communication (SNC) concept as described in the SAP NetWeaver Security Guides. Note the following restriction:

IDoc communication uses logical ports. If these are SAP systems, the SNC concept also applies here. If these are not SAP systems, separate precautionary measures (access control at directory level and so on) are to be taken.

We do not ship any RFC connections. Before you configure internal non-local data flows, read the information in the SAP NetWeaver 7.10 Security Guides. However, the following RFC connections have to be configured to operate Bank Analyzer. Do not create the users belonging to these as dialog users.

- RFC communication for Tool BI.
- RFC communication within Tool BI (RFC call in the BI standard client): see SAP Note 631416.
- RFC communication in the context of after import methods of the client copy. The relevant authorization objects are: S_TABU_DIS, S_RS_ICUBE, S_RS_ADMWB, S_RS_ISOUR, S_BTCH_ADM, S_ADMI_FCD, S_BTCH_JOB, S_RS_ODSO, and S_RS_ISET.

External Data Flows

External data flows are those whose source or destination is not Bank Analyzer.

Bank Analyzer uses SAP standard interface technology only. It does not have its own concepts. The interfaces must be protected as described in the SAP NetWeaver 7.10 Security Guides.

Note that Bank Analyzer does not ensure the security of the external parts. Bank Analyzer can ensure the security of external data flows into the interface in question only if Bank Analyzer is the source of the data flow. Bank Analyzer can ensure the security of external data flows from the interface in question if Bank Analyzer is the destination of the data flow.

Bank Analyzer can handle the following interfaces:

3. **BAPIs:**

   BAPIs are used to supply data from the operational feeder systems or other external providers to the SDL, RDL, and Historical Database (HDB).

   You can use transaction BAPI to obtain a list of other BAPIs. Here you can also find documentation that refers to the associated authorization objects.

   Some BAPIs are named by Bank Analyzer processes. In this case, the data flows are internal data flows, such as those that occur when the HDB is used to generate scenario data in the SDL.

   The BAPIs in the SDL apply the same authorization checks as those used when data is processed manually. **Exception**: The "complex authorization check" is not carried out for automatic data imports.

   BAPIs and the standard BI data acquisition function can be used to supply Tool BI with information. See also the SAP Business Information Warehouse Security Guides.

4. **Enterprise Services:**

   Bank Analyzer contains inbound services for importing and reversing results in the RDL (for example, subledger documents, fair values, funds transfer pricing rates) and

SDL (for example, master data and flow data for loans and accounts) as well as outbound services (for example, for sending general ledger documents to GL).

You can display an overview of the XI services by calling transaction SPROXY. The Bank Analyzer software component is referred to here as FSAPPL, namespaces http://sap.com/xi/BA/Global and http://sap.com/xi/BA.

5. **Files:**

   Files can be used as follows:

   - Input:
     - The communication framework (primary data source) in the SDL enables each Bank Analyzer core process to access external files.
     - You can use SAP NetWeaver BI to import files.

       You can use this function in Tool BI to load master data such as texts, attributes, and hierarchies for characteristics.

       You can use this function in Reporting BI to load master data and transaction data to add to the data extracted from Bank Analyzer.
     - The DX Workbench can be used to import files and call BAPIs.
     - In systems that are not live production systems, you can import Excel files containing test data for accounting. The method is additionally secured by authorizations. You should use the functions of the SDL rather than the interface.
     - The HDB contains a GUI upload that you can use to import text files or XML files into the data processing storage area of the HDB.
     - To switch to the subledger scenario you can use transaction /BA1/B0_CMS_TAB_EXP (Data Export to XML File).
   - Output:
     - Bank Analyzer Core contains functions for operational reporting based on the lists in ABAP List Viewer (ALV). It also contains a download function for data that has already been displayed.
     - Bank Analyzer Core contains different processes (such as the SDL data export, and the interface for reporting) that can be used to export data in files.
     - If Bank Analyzer data can be archived, the standard tool Archive Development Kit (ADK) is used to do this. The data that is to be archived is written to files.
     - The open hub interface in SAP NetWeaver BI SAP BW uses files to extract the data stored in BI.
     - The front-end (MS Excel, Internet browser) in which reports were generated in Reporting BI can be used to download the reports to a file.
     - The HDB run for supplying models with data can use an outbound BAPI to transfer the data to bank-internal models (see also the documentation for the InputWrite method of the InternalModelHDB business object, and the documentation for Business Add-In (BAdI) /BA1/R6_INTERNAL_MDL). Define the transfer process (and the use of confirmation prompts) in the BAdI implementation
     - The HDB contains a GUI download that you can use to export Bank Analyzer data in text files or XML files. You can use the data processing framework of the HDB to select the data (from the SDL, HDB, or the Analyzers) and, if required, modify it before you download it.

- To switch to the subledger scenario you can use transaction /BA1/B0_CMS_TAB_EXP (Data Export to XML File).

In all these cases, the files are beyond the scope of the mechanisms provided by SAP for data security (authorizations, and so on). Therefore, the customer alone is responsible for the security of the files and of the confidential data contained therein.

The Basis authorization object S_DATASET can be used to define the access to files from the SAP back-end system. You should use this authorization object to restrict access to files.

The data acquisition function in SAP NetWeaver BI can be secured for Tool BI and Reporting BI as described in the SAP Business Information Warehouse Security Guides.

In this case, Bank Analyzer does not ensure data quality or the security of the data sources; you have to handle these issues separately.

- **RFC:**

  You can use RFC modules to supply the RDL with data from your operational systems, or from external providers. These RFC modules of the RDL apply the same authorization checks as those used when results data is processed manually.

  You can also use RFC connections to import limits into Limit Manager. Authorization objects in Limit Manager can be used for data security purposes.

  The Fair Value Server in Bank Analyzer uses a hard coded RFC connection 'ADS' for the connection to AdobeService. See also notes 834573 *SAP Interactive Forms by Adobe: Acrobat/Reader Version* or 894009 *Adobe Document Services: Configuration Guide (SAP NW7.0)* or 1172167 *Central Note for ADS on NW70 EhP1*.

Additional Communication Channels

It is also possible to display or call reports and other transactions in SAP Enterprise Portal. SAP Enterprise Portal is to be secured following SAP standards.

4.4 Security of the Data Backup

Bank Analyzer data is saved in the system database. There are no additional requirements to those described in the SAP NetWeaver 7.10 Security Guides.

No data is stored temporarily in other locations. You must differentiate between Customizing and application data:

- Customizing data is created, changed, or deleted manually during the implementation phase, and sometimes after the system has gone live. Transports are used for live systems.

  If the components in Bank Analyzer Core contain deletion reports, access to these is protected by the authorization concept or they check whether the system is flagged as a production system. If the system is a production system, the program is not executed.

- Application data is imported into the SDL from the operational system and processed automatically. The SDL also contains functions for processing data manually. These functions have to be protected by means of the authorization concept. Changes to data in the SDL are recorded by a technical time stamp. Corrections can also be recorded by the correction server. Processing results that can be used are saved in the RDL; processing results that are specific to an Analyzer are either stored in the RDL (for example, ALM results) or the Analytics Layer. Depending on the solution, there are functions for posting, correcting, reversing, reorganizing, deleting, and archiving the results data that has been stored. These functions are protected by the authorization concept. For more information, see the documentation for these functions.

SAP Accounting for Financial Instruments contains report BA1/RB1_TT_DELETE_APP_DAT that can delete selected application data. This report cannot be used in production systems.

The software delivered does not contain any default settings for the protection of Customizing data or application data. You must set the level of protection that is necessary by assigning authorization to users and by entering system settings (for example, to define whether the data in a given client can be changed).

4.5 User Interface

Bank Analyzer Core uses the standard SAP GUI. ITS cannot be used.

Depending on how the reporting function was implemented, an Internet browser can also be used as the user interface for Reporting BI. This has to be protected in accordance with the SAP Business Information Warehouse Security Guides.

4.6 User Administration and Authentication

Technical users and dialog users are used in Bank Analyzer. Only the standard users described in the SAP NetWeaver 7.10 Security Guides are delivered in the system. All users are created by customers' own system administration teams. These teams are also responsible for defining the start identification parameters, such as the password.

The application accepts SAP logon tickets and digital certificates (X.509).

Roles

The Bank Analyzer component contains a range of roles. These roles are given as examples that must be adapted. Do not use them in your production system in the form in which they are delivered.

All authorization objects that are maintained in these roles have been added manually. For creating your own roles you can use the templates roles or use transactions SU24/SU25 with transaction PFCG and dynamic role creation respectively.

The SAP_BA1_TECH_*-roles (as listed below) contain authorizations with ‘*’-values for the authorizations. Such ‘*’-authorizations are critical because they allow unrestricted access to data or activities.

Authorization object S_RFC is maintained in the delivered template roles with explicitly listing RFC function modules or function groups respectively. Not all RFC function modules are protected with explicit internal authorization checks. So because of this, and due to the general criticality of RFC function modules, do not provide S_RFC with ‘*’-authorizations.

You can display the roles available by using Profile Generator (transaction PFCG) in the system. Use Profile Generator to create additional own roles.
The example roles are organized as follows:

By types of users:

- SAP_BA1_SHOW_* Example roles for display users
- SAP_BA1_USER_* Example roles for standard users (applications)
- SAP_BA1_TECH_* Example roles for technical users (applications)
- SAP_BA1_EXPERT_* Example roles for business experts (Customizing and applications)
- SAP_BA1_ADM_* Example roles for administrators for the areas BW, FDB/SDL, RDL and RR

By Bank Analyzer areas/ applications:

The central paths on the *SAP Easy Access* screen are listed below, together with the roles. All menu paths start as follows: *Financial Services -> Bank Analyzer*.

- SAP_BA1_*_BW Example roles for the usage of the Tool BI
- SAP_BA1_*_FDB Example roles for Source Data Layer *Source Data Layer*
- SAP_BA1_*_RDL Example roles for Result Data Base *Results Data Layer*
- SAP_BA1_*_LM Example roles for Limit Manager *-> Analytics -> Limit Manager*
- SAP_BA1_ *_ALM Example roles for the Bank Analyzer part of Asset Liability Management *Interfaces to Other Applications -> Data Supply for ALM*
- SAP_BA1_*_CE Example roles for Credit Exposure *-> Processes and Methods -> Credit Risk -> Credit Exposure*
- SAP_BA1_*_CPM Example roles for Credit Portfolio Management *-> Processes and Methods -> Credit Risk -> Credit Portfolio Data Processing*
- SAP_BA1_*_CRST Example roles for Credit Risk Analysts
- SAP_BA1_*_DR Example roles for Generic BW extraction -> Infrastructure -> Extraction and Reporting Services -> Generic BW Data Extraction
- SAP_BA1_*_GEM Example roles for General Business Methods *-> Processes and Methods -> General Calculation and Valuation Methods*
- SAP_BA1_*_HDB Example roles for Historical Database *-> Analytics -> Historical Database*

- SAP_BA1_*_HM Example roles for Hedge Management Analysis
  -> Processes and Methods -> Hedge Processes
- SAP_BA1_*_RB Example roles for Risk Basis
  -> Processes and Methods -> General Calculation and Valuation Methods -> Present Value Calculation
- SAP_BA1_*_RR Example roles for Regulatory Reporting
  -> Analytics -> Regulatory Reporting Interface
- SAP_BA1_*_Imp* Example roles for Impairment as part of Financial Accounting for Banks
- SAP_BA1_*_PAIA_AL Example roles for General Ledger Connector and Financial Statement Preparation;
  -> Analytics -> General Ledger Connector;
  -> Analytics ->Financial Statement Preparation
  for the General Ledger, see the SAP ERP Security Guides
- SAP_BA1_*_PAIA_PML Example roles for Accounting and Profitability
  -> Analytics -> Profit Analyzer;
  -> Processes and Methods -> Accounting for Financial Products

Example Roles

Role	Description
SAP_BA1_SHOW_ALM	Display Authorization for Asset Liability Management
SAP_BA1_USER_ALM	Application Authorization for Asset Liability Management
SAP_BA1_TECH_ALM	Technical Role for Asset Liability Management
SAP_BA1_EXPERT_ALM	Customizing and Application Authorization for Asset Liability Management
SAP_BA1_SHOW_BW	Authorizations for Displaying Data in the BW Area
SAP_BA1_USER_BW	Authorizations for Reporting in the BW Area
SAP_BA1_TECH_BW	Reporting Authorizations for the BW Area
SAP_BA1_EXPERT_BW	Modeling and Reporting Authorizations for the BW Area
SAP_BA1_ADM_BW	Administrator Authorizations for the BW Area
SAP_BA1_SHOW_CE	Authorization for Displaying Data in Credit Exposure

SAP_BA1_USER_CE	Application Authorization for Credit Exposure
SAP_BA1_TECH_CE	Technical Role for Credit Exposure
SAP_BA1_EXPERT_CE	Customizing and Application Authorization for Credit Exposure
SAP_BA1_SHOW_CPM	Display Authorization for Credit Portfolio Management
SAP_BA1_USER_CPM	Application Authorization for Credit Portfolio Management
SAP_BA1_TECH_CPM	Technical Role for Credit Portfolio Management
SAP_BA1_EXPERT_CPM	CPM Customizing and Application Authorization
SAP_BA1_NWBC_CRST	NetWeaver Business Client Role for Credit Risk Analysts
SAP_BA1_SHOW_CRST	Display Role for Credit Risk Analysts
SAP_BA1_USER_CRST	User Role for Credit Risk Analysts
SAP_BA1_EXPERT_CRST	Expert Role for Credit Risk Analysts
SAP_BA1_SHOW_DR	Authorization for Displaying Data for Generic BW Extraction
SAP_BA1_USER_DR	Application Authorization for Generic BW Extraction
SAP_BA1_TECH_DR	Technical Role for Generic BW Extraction
SAP_BA1_EXPERT_DR	Application/Customizing Authorization for Generic BW Extraction
SAP_BA1_SHOW_FDB	Authorizations for Displaying Data in the SDL Area
SAP_BA1_USER_FDB	Application Authorizations for the SDL Area
SAP_BA1_TECH_FDB	Application Authorizations for the SDL Area
SAP_BA1_EXPERT_FDB	Customizing Authorizations for the SDL Area
SAP_BA1_ADM_FDB	Administrator Authorizations for the SDL Area
SAP_BA1_SHOW_GEM	Display Authorization for General Business Methods
SAP_BA1_USER_GEM	Application Authorization for General Business Methods
SAP_BA1_TECH_GEM	Technical Role for General Business Methods
SAP_BA1_EXPERT_GEM	Application and Customizing Authorization for General Business Methods
SAP_BA1_SHOW_HDB	Authorization for Displaying Data in the Historical Database

SAP_BA1_USER_HDB	Application Authorization for the Historical Database
SAP_BA1_TECH_HDB	Technical Role for HDB
SAP_BA1_EXPERT_HDB	Customizing and Application Authorization for HDB
SAP_BA1_SHOW_HM	Display Authorization for Hedge Management
SAP_BA1_USER_HM	Application Authorization for Hedge Management
SAP_BA1_TECH_HM	Application Authorization for Hedge Management
SAP_BA1_EXPERT_HM	Customizing and Application Authorization for Hedge Management
SAP_BA1_SHOW_LM	Authorization for Displaying Data in Limit Manager
SAP_BA1_USER_LM	Authorization for the Limit Manager Application
SAP_BA1_TECH_LM	Authorization for the Limit Manager Application
SAP_BA1_EXPERT_LM	Customizing and Application Authorization for Limit Manager
SAP_BA1_SHOW_PAIA_AL	Display General Ledger Connector and Financial Statement Preparation
SAP_BA1_EXPERT_IMPRMT	Authorization for Customizing and Application Authorization for Impairment Functions
SAP_BA1_USER_IMPRMT	Authorization for Customizing (Display) and Application Authorization (Execution) for Impairment Functions
SAP_BA1_SHOW_IMPRMT	Authorization for Customizing and Application Authorization for Impairment Functions, Display Only
SAP_BA1_USER_IMPRMT_ WEBSERVICE	Authorization for Synchronous Impairment - SOA Services
SAP_BA1_TECH_IMPRMT_WEBSERVICE	Authorization for asynchronous Impairment - SOA Services
SAP_BA1_USER_PAIA_AL	User for General Ledger Connector and Financial Statement Preparation
SAP_BA1_TECH_PAIA_AL	User for General Ledger Connector and Financial Statement Preparation
SAP_BA1_EXPERT_PAIA_AL	Experts in General Ledger Connector and Financial Statement Preparation
SAP_BA1_SHOW_PAIA_PML	Display Accounting and Profitability Analysis
SAP_BA1_USER_PAIA_PML	User for Accounting and Profitability Analysis
SAP_BA1_TECH_PAIA_PML	User for Accounting and Profitability Analysis
SAP_BA1_EXPERT_PAIA_PML	Experts in Accounting and Profitability Analysis

SAP_BA1_SHOW_RB	Authorization for Displaying data in Customizing/Application for Risk Basis
SAP_BA1_USER_RB	Authorization for Users for Customizing/Application for Risk Basis
SAP_BA1_TECH_RB	Authorization for Users for Customizing/Application for Risk Basis
SAP_BA1_EXPERT_RB	Authorization for Expert Users for Customizing/Application for Risk Basis
SAP_BA1_SHOW_RDL	Display Authorizations for the RDL Area
SAP_BA1_USER_RDL	Application Authorizations for the RDL Area
SAP_BA1_TECH_RDL	Application Authorizations for the RDL Area
SAP_BA1_EXPERT_RDL	Customizing Authorizations for the RDL Area
SAP_BA1_ADM_RDL	Administrator Authorizations for the RDL Area
SAP_BA1_SHOW_RR	Authorization for Displaying Data in Regulatory Reporting
SAP_BA1_USER_RR	Authorization for Changing Data in Regulatory Reporting
SAP_BA1_TECH_RR	Technical Role for Regulatory Reporting
SAP_BA1_EXPERT_RR	Expert Authorization for Regulatory Reporting
SAP_BA1_ADM_RR	Administration Authorization for Regulatory Reporting

To add missing authorizations to role SAP_BA1_EXPERT_FDB, see SAP Note 1378033.

Users

No users are delivered with Bank Analyzer. Use transaction SU01 (User Maintenance) to create users.

The Bank Analyzer roles do not contain all the authorizations necessary to execute basic functions in an SAP system. Therefore, every user needs these basic authorizations in addition to the authorizations for the respective Bank Analyzer role. For more information about user management for SAP NetWeaver, see the SAP NetWeaver Security Guide.

If want a user that processes the Reporting & Analytics Layer or the Calculation & Valuation Layer to be able to display the underlying source data, you need to assign role **SAP_BA1_SHOW_FDB** to this user, in addition to his or her role for this layer.

If a Bank Analyzer user needs to be able to perform generic BI extraction, you need to assign role **SAP_BA1_*_DR** to this user, in addition to his or her Bank Analyzer role.

For the generic BI extraction started in Reporting BI to extract data from Bank Analyzer, a batch user has to be created in Bank Analyzer with role SAP_BA1_TECH_CR. This user has to be assigned to be used in the generic BI extraction in Reporting BI.

Note that due to the generic nature of the characteristic and key figure repository, the authorizations in Bank Analyzer roles need to be adjusted to your implementation. Therefore, you might need to specify in your authorizations the names and values of characteristics, key figure, and structures generated from them.

For more information about authorizations for generic BI extractions, see SAP Note 1373479.

Characteristic-Based Authorizations

Bank Analyzer contains freely definable characteristics. In all Bank Analyzer components, you have to make certain authorizations dependent on the characteristic values. This also applies to the characteristics you create yourself (custom characteristics).

Bank Analyzer is designed so that the combination of (custom) characteristics assigned to the fields of the predefined authorization objects is variable. Special Customizing is used to assign the characteristics to the fields in the authorization objects. For more information, see the Bank Analyzer section of SAP Library. This is an extension to the standard SAP authorization concept, and not specific to Bank Analyzer.

Use this function for employee accounts. For example, those accounts that you want to identify as such by means of a characteristic, and then make access to these accounts subject to special authorization. You can also create organizational units as characteristics, which can then be used to restrict access to Customizing and application data.

Information Specific to the Drill-Through Function in Reporting BI

When users drill through data from reports generated in Reporting BI, a process that uses the report-report interface (see also the BI Content section of SAP Library), to Bank Analyzer Core, they have to log on to Bank Analyzer Core. A dialog user is required for the drill-through function, whereas a batch user is enough for the technical extraction. Note that the authorizations you assign in Reporting BI are independent of those you assign in Bank Analyzer Core.

Make sure that the authorizations you assign in Reporting BI and Bank Analyzer Core are consistent. In this way you avoid permitting access to certain data in one system, and preventing access to the same data in another system.

Make sure that the authorizations you assign for navigation targets in Bank Analyzer Core are the same as those in Reporting BI.

Source Data Aggregation (SDA)

If a process uses source data aggregation (such as create, read), the authorization object F_BAHW_RES is checked. Field /BA1/HWRDA (results data area) must always be “1SDA”. Field /BA1/HWRT (result type/view) always has the prefix “1S_”, so you should apply “1S_*” because the result types for aggregation are generated in the system and the names are not known when the roles are created. Field ACTVT (activity) can have the values 01 (create), 03 (display), and 85 (cancel/reverse). If you use a process with SDA, make sure that the user has the abovementioned authorizations.

4.7 Other Security Information

Working in the SAP Development Environment

Note that access to the SAP development environment should be highly restricted. Users with authorization for developing, debugging, and changing the contents of fields in the debugger, can potentially read, change, or delete any information in Bank Analyzer. For example, they can change information by calling the relevant BAPI and circumventing the programmed authorization checks. These users can also modify system parameters.

For information about how you can prevent unauthorized access to the SAP development environment, see the SAP NetWeaver 7.10 Security Guides.

Assign development authorization to as few users as possible. Make sure that the processes you use in your organization (principle of dual control, code reviews) do not permit coding to get into the production system without first being checked. A simple test of the coding in the test system is not sufficient since it is possible to let harmful code sequences run only in production systems.

Also, see SAP Note 1594110 concerning code injection vulnerability in Function and Class Builder. Authorization object S_DEVELOP is needed for segmentation services.

Openness, User Exits, and the Integration of User-Defined Function Modules in Bank Analyzer Tools

Bank Analyzer has an extensive enhancement concept, which offers user exits at suitable points, in the form of BAdIs.

The tools in Bank Analyzer (such as the derivation tool and the module editor) can be used to access function modules. Depending on the application, you can add your own custom function modules.

In both cases, you can use all the functions of the ABAP Workbench. This means that (unlogged) read or change access to all system parameters and all information in Bank Analyzer is potentially possible. We do not guarantee the security of non-SAP implementations, enhancements, or modifications. We cannot provide any technical protection against this type of improper use.

Formula and Condition Step Types in the Module Editor

The module editor interprets the Customizing settings that were entered and uses these to generate code. For example, you can enter any ABAP statements in the *Formula* and *Condition* and loop step types provided each statement has correct syntax and finishes with a period. You can use all the functions of the ABAP Workbench.

However, the use of these module editor step types in this format has not been released by SAP.

The Customizing settings in the module editor are protected by development authorization object S_DEVELOP with activity ACTVT = 02, object type OBJTYPE = PROG and object

name OBJNAME = FS-BA-MODULE-EDITOR. Only users with this authorization are allowed to create and change the coding sequence.

The module editor contains a test function. This function enables you to test modules that have not been activated. It is therefore conceivable to create, execute, and remove coding sequences as described. Since this means that all ABAP Workbench functions can be used, the module editor must never be released for Customizing in the production system. It is possible to cause extensive damage in the development or test system. See SAP Note 676390, which contains information about Customizing and transports for the module editor.

Make sure that the processes you use in your organization (principle of dual control, code reviews) do not permit modules to get into the production system without first being checked. A simple test of the Customizing settings in the test system is not sufficient since it is possible to let harmful code sequences run only in production systems.

Data Aggregation in the Historical Database/Descriptive Statistics

Data is aggregated in the HDB. In these processes, data is compressed. This can be for the purpose of calculating descriptive statistics, for example. During aggregation, authorization checks may not be effective.

This is the case when a user is not authorized to display data records for certain characteristics (category A characteristics) if these data records contain particular characteristic values for which he or she is not authorized. These constraints do not apply to other characteristics (category B characteristics).

If the user then starts data aggregation, and the results of aggregation are only noninitial characteristic values for category B characteristics, the user is able to display the results.

If the user also enters selection criteria for category A characteristics, these criteria are not checked. If the user chooses particular single values, he or she is able to draw conclusions about the single values just by displaying the aggregated result.

The characteristic *Business Partner* is a category A characteristic. Our example user is not authorized to display business partner BP1. Business partner BP1 belongs to sector S1. The characteristic *Sector* is a category B characteristic, which means that there are no constraints for sectors.

This means that any user can display data summarized on the basis of the *Sector* characteristic, which would include data aggregated at business partner level.

Our example user now selects for the aggregated report only the data for business partner BP1. Although the results do not mention the business partner explicitly, they still contain the values for BP1. There is no entry in the *Business Partner* field, but a data record for sector S1 is displayed, and this record contains the aggregated values for business partner BP1. In this way, our example user can determine the total sales of business partner BP1, for example.

4.8 Trace Files and Log Files

In the subledger scenario, financial accounting and cost accounting use the Calculation and Valuation Manager (CVPM) tool and its application log management, with a few exceptions. In the merge scenario, the process standard framework is used with the application log. In principal, the application log is used in each process. Due to the large number of messages in an application log (>100,000), an analysis tool was created to simplify the analysis of messages and errors. The application log contains mainly messages that affect the editing of processes. Characteristic values that draw conclusions about data are issued only if an error situation arises. However, only data that does not draw conclusions about the characteristic values of the complete transaction is issued. The financial positions have two-dimensional version management in part of their data. All flow data (documents) cannot be deleted but can be only reversed or archived. This enables continuous version management. The system does not write change documents for the documents because the original documents already have this function in full and this ensures that all data can be traced.

In this context, Basel II calculation and the general methods use the application log, which is accessed via run management. Depending on the filter settings, a large number of messages might be generated. They can be analyzed using a tool in run administration. The application log contains mainly messages that affect the editing of processes. Characteristic values that draw conclusions about data are issued only if an error situation arises. However, only data that does not draw conclusions about the characteristic values of the complete transaction is issued. There is a run concept for the results data in the RDB: This means that a separate RDB area is used for each run. The following applies to results data in the RDL: There are views of runs, data in the same results data area (RDA) on the same key date can be stored in two dimensions, and single results can be reversed. Using two-dimensional version management, you can trace the status both before and after reversal.

The RDL does not have a trace file or a log file.

Import of data to the SDL: If the Bank Analyzer BAPIs are used directly as intended, the system does not write any log data. However, if the BAPIs are not called directly, but are used via the data transfer workbench (SXDA), the log functions available there can be used. These are non-Bank Analyzer log functions.

Tracing of authority groups: A change document is created when the authority group of a financial transaction or instrument is changed. To improve performance, this is not done when a financial transaction or instrument is created.

The hedge processes (fair value effectiveness test, cash flow hedge analysis, hedge accounting workplace, portfolio items) use the application log directly. Depending on the filter settings, a large number of messages might be generated. They can be analyzed using a tool in run administration. The application log contains mainly messages that affect the editing of processes. There is a run concept for the results data in the RDB: This means that a separate RDB area is used for each run.

Only relevant for customers of Strategy Analyzer: Strategy Analyzer uses the application log directly. Depending on the filter settings, a large number of messages might be generated. They can be analyzed using a tool in run administration. The application log contains mainly messages that affect the editing of processes. There is a run concept for the results data in the RDB: This means that a separate RDB area is used for each run.

For logging and tracing (for example, in the Integration Engine or Post Processing Office) of data transferred via service interfaces, see the SAP NetWeaver Security Guide.

5 Business Partner for Financial Services

5.1 User Administration and Authentication

Roles

The Business Partner for Financial Services (FS-BP) component contains several user roles. These roles are given as examples that must be adapted. Do not use them in your production system in the form in which they are delivered.

Authorization objects used in these roles have been added manually. To create your own roles, you can use the template roles or use transactions su24/su25 with transaction PFCG and dynamic role creation respectively.

The SAP_CA_BP_DEVELOPER_AG role (as listed below) contains '*' values for authorizations. These '* authorizations are critical because they allow unrestricted access to data or activities.

You can display the roles available by using the Profile Generator (transaction PFCG) in the system. You can also use the Profile Generator to create your own additional roles.

In a multi-system landscape for banking consisting of CRM, FSP and ERP instances, user management is important. Different user groups exist and need authorizations according to their roles.

The following **template roles** are available for the operational Business Partner:

Role	Description
SAP_CA_BP_CUSTOMIZER_FS	SAP Business Partner: Customizing
SAP_CA_BP_DEVELOPER_AG	SAP Business Partner: Developer with enhancement options in BDT framework
SAP_CA_BP_MAINTAIN_FS	User role for Business Partner data maintenance
SAP_CA_BP_DISPLAY_FS	User role to display Business Partner data
SAP_CA_BP_ADMIN_FS	User role for the administration of Business Partner data
SAP_CA_BP_CLEANS_CREAT_FS	Business Partner user with authorization to create cleansing cases
SAP_CA_BP_CLEANS_EXPERT_FS	Business Partner user with authorization to process cleansing cases

The following **template roles** are available for the analytical Business Partner (Bank Analyzer):

Role	Description
SAP_BA_BP_FS_CUSTOMIZER	Role to customize Business Partner in analytical systems
SAP_BA_BP_FS_EXPERT	Expert role to correct Business Partner data in analytical systems

If a user role is needed to display analytical business partner data, the display permissions of role SAP_BA_BP_FS_EXPERT can be used (permission for transaction BPV3, BPV3s, and

BPV4s).

Basic Authorizations

The business partner template roles do not contain authorizations necessary to execute basic functions in an SAP system. Therefore, every user needs basic authorizations in addition to the authorizations for the respective business partner role.

Basic authorizations are required, for example, for the different channels such as S_GUI for SAPGUI channel, S_RFC for remote communication using RFC protocol and S_SRT* for service communication. For more information about basic authorizations and user administration for SAP NetWeaver, see the SAP NetWeaver Security Guide.

Users

No users are delivered with Business Partner for Financial Services. Use transaction SU01 (User Maintenance) to create users.

5.2 Authorizations

Authorization objects

The following authorization objects exist in the Business Partner for Financial Services area:

Object	Description
B_BUPA_ATT	Business Partner: Authorization Types
B_BUPA_FDG	Business Partner: Field Groups
B_BUPA_GRP	Business Partner: Authorization Groups
B_BUPA_RLT	Business Partner: BP Roles
B_BUPA_PGM	FS Business Partner Custom Grouping
B_BUPR_BZT	Business Partner Relationships: Relationship Categories
B_BUPA_CRI	FS Business Partner: BP Role Cat./Differentiation Criterion
B_BUPR_FDG	Business Partner Relationships: Field Groups
B_BUPA_SLV	Selection Variant for Total Commitment
B_CCARD	Payment Cards
B_CARD_SEC	Authorization Encryption Card Master

For more information about the authorization objects, see the online documentation in transaction SU21.

Employees, VIPs and other restricted groups of business partners should be secured by own groups. Restrictions are possible using field AUGRP in table BUT000 (authorization object B_BUPA_GRP) or field GROU_FEATURE in table BP001 (authorization object B_BUPA_PGM).

The authorization objects B_BUPA_GRP and B_BUPA_PGM are checked in the channels SAPGUI, BAPI and services.

, A separate authorization object (B_CCARD) exists for payment cards. You can use this object to grant different authorizations for creating, displaying or changing payment card data. In addition, you can use authorization object B_CARD_SEC to control the encryption or decryption of payment card data.

In the SAP GUI channel, payment card information can be masked.
For more information, see http://service.sap.com/securityguide → *SAP Business Suite Applications* → *SAP CRM* → *Security Guide for SAP CRM 7.0.*

For more information, see help.sap.com/crm → Basic Functions →Payment Card Processing → Security for Payment Card Data.

In the SAP GUI channel, you can use the authorization object B_BUPA_FDG for UI-channel--specific detailed checks at BDT field-group level.

You can also check at a more detailed level in the service channel,. To do so, you have to define your own authorization objects. The corresponding checks must be implemented in the enhancement BAdIs of the Business Partner services.

5.3 Tracking of Changes

Changes to business partner data are tracked using change documents. The business processes that lead to business partner data changes are tracked using BPCA (Business Process Chain Assignment) and the Process Journal.

Tracking of business processes using BPCA is currently available with the business partner for banking in the service channel in the Banking Services Platform. Limitations exist with BPCA in the replication scenario, meaning BPCA information is not replicated.

5.4 Integration Scenarios

5.4.1 Maintenance Scenario

In a multi-system landscape it is assumed that one business partner instance is defined as master and other instances as clients. We recommend that you maintain business partner data in the master instance using template role SAP_CA_BP_MAINTAIN_FS and allow users in client instances to display business partner data using template role SAP_CA_BP_DISPLAY_FS.

5.4.2 Replication Scenario

In the replication scenario, changes to business partner data are replicated from the business partner master instance to the client instances. In the replication clients, technical users in combination with individual users can be used to process replication messages and to update business partner records in replication clients. You can use the role SAP_CA_BP_MAINTAIN_FS as a template for any business partner maintenance authorizations that you need.

5.4.3 Non-Replication Scenario

In the non-replication scenario, business partner data is not stored in the non-replication client instance, but retrieved from the master instance when needed. Users working with the non-replication client instance need authorization to retrieve business partner and relationship data in the business partner master instance using services. You can use the role SAP_CA_BP_DISPLAY_FS as a template.

If you want to implement the process to terminate business partner roles or to add alias names in the non-replication scenario, a technical user is needed in the master instance who is authorized to update business partner data using services. You can use the role SAP_CA_BP_MAINTAIN_FS as a template.

In a non-replication client, a technical user is needed to process information messages and to raise business partner and relationship events. When information messages are processed, the authorization objects B_BUPA_GRP, B_BUPA_PGM and B_CCARD are checked.

5.4.4 Integration Operations & Analytics Scenario (IOA)

Operational and analytical business partner data is integrated using information messages that are sent periodically from the business partner master instance to the IOA client instance (Bank Analyzer). A technical user in combination with individual users can be used to process business partner and relationship information messages and to update the analytical business partner data in Bank Analyzer. When information messages are processed, the authorization objects B_BUPA_GRP and B_BUPA_PGM are checked. >You can use the role SAP_BA_BP_FS_EXPERT as a template for any analytical business partner maintenance authorizations that you need.

5.4.5 Data Cleansing Scenario

The data cleansing scenario is used to identify and merge business partner duplicates. Users who work with this scenario need specific authorizations to create and process cleansing cases.

You can use the role SAP_CA_BP_CLEANS_CREAT_FS as a template for users to create and display cleansing cases only. This role also contains authorizations to display business partner data.

You can use the role SAP_CA_BP_CLEANS_EXPERT_FS as a template for data cleansing experts to create and process cleansing cases. This role contains comprehensive cleansing case authorizations and maintenance authorizations for business partner data. Business partner maintenance authorizations are needed while processing cleansing cases.

6 Transaction Banking

6.1 Deposits Management

6.1.1 Authorizations

If the user in question is to use dialog transactions only, assign the following authorization objects to the user:

Authorization Object	Description
F_CN_FDG	FS-AM Contract: Field Groups
F_CN_MOD	FS-AM Contract: Contract Element
F_CN_ORG	FS-AM Contract: Managing Org. Unit and Product Category
F_EODP_ACT	FS-AM End-of-Day Processing
F_PIT_TRT	FS-AM Payment Item: Transaction Type

If the user in question is to use cross-system functions (technical user), assign the following authorization objects to the user in addition:

Authorization Object	Description
F_CN_ACT	Simplified Contract Authorization Check
F_CN_BAPI	FS-AM Simplified Authorization Check in BAPIs

To obtain a role to enable the user to use dialog transactions for deposits management, assign the following transactions to it:

- BP
- BCA_DATE_POST_SET
- BCA_DATE_EOD_SET
- BCA_CN_ACCT_01
- BCA_CN_ACCT_02
- BCA_CN_ACCT_03
- BCA_ACC_MST_RUN
- BCA_CN_KFG
- BCA_PO_FO_MULTI
- BCA_ACBAL_NEXT_DATE
- BCA_PAYMITEM_CREATE
- BCA_PAYMITEM_MAINTN
- BCA_ACBAL_ACC_S

Make sure that the authorization objects mentioned above are included and equipped with full authorization. Note that a role with full authorization is highly critical and should be used only for demonstration purposes and not for productive usage.

To obtain a role to enable the user to use cross-system functions (technical user), add the authorization objects mentioned above manually to the role created for dialog transactions.

Additional authorization checks are available in the master contact application facilities. These authorization checks are not performed by default, but can be switched on using the scenario definition /FSFAC/SD_AL_FAC_1 in the framework for Switchable Authorization Check Scenarios (SACF) to configure the additional set of authorization checks during processes relevant for master contract application facilities (see note 2285741 for further details).

6.2 Loans Management

6.2.1 Authorizations

If the user in question is to use dialog transactions only, assign the following authorization objects to the user:

Authorization Object	Description
F_BODB_FCT	FS-AM Disbursement: Operation
F_BODB_ORG	FS-AM Disbursement: Organizational Unit Managing Contract
F_BODB_RSN	FS-AM Disbursement: Disbursement Reason
F_BORN_FCT	FS-AM Renewal : Operation
F_BORN_ORG	FS-AM Renewal : Organizational Unit Managing Contract
F_BOTC_FCT	FS-AM Account Closure: Operation
F_BOTC_ORG	FS-AM Account Closure: Contract-Managing Organizational Unit
F_BOTC_RSN	FS-AM Account Closure: Notice Reason
F_BOPF_FCT	FS-AM Loan Payoff: Operation
F_BOPF_ORG	FS-AM Loan Payoff: Organizational Unit Processing Contract
F_BOPF_RSN	FS-AM Loan Payoff: Reason
F_CN_FDG	FS-AM Contract: Field Groups
F_CN_MOD	FS-AM Contract: Contract Element
F_CN_ORG	FS-AM Contract: Managing Org. Unit and Product Category
F_EODP_ACT	FS-AM End-of-Day Processing
F_FICO_IND	FICO Individual Conditions
F_PIT_TRT	FS-AM Payment Item: Transaction Type
F_BL_BLCAT	Authorization Check API (Billing Category and Activity)
F_FSPD_ACT	Authorization Object for Payment Distribution
F_FSPD_DIR	Authorization Object for Payment Distribution Directives
F_BORN_ACT	FS-AM Renw : Activity (API)
F_DEHDOCAC	FS-AM-PLM: Document Category 0001 (Account)
F_DEHDOCBP	FS-AM-PLM:PLM Doc. Category 0002 (Card), 0003 (Bus. Partner)
F_DEH_BGRP	FS-AM-PLM: Entry Origin
F_CN_ACT	FS-AM Simplified Authorization Check in BAPIs
PLOG	Personnel Planning

If the user in question is to use cross-system functions (technical user), assign the following authorization objects to the user in addition:

Authorization Object	Description
F_BODB_ACT	FS-AM Disbursement: Activity (API)
F_BOPF_ACT	FS-AM Loan Payoff: Activity (RFC)

F_BOTC_ACT	FS-AM Account Closure: Activity (BAPI)
F_BODF_ACT	FS-AM Deferral : Activity (API)
F_CN_BAPI	FS-AM Simplified Authorization Check in BAPIs
F_FICO_AIN	FICO Individual Condition BAPIs
F_BL_ACTVT	Authorization Check BAPI (Activity Only)

To obtain a role to enable the user to use dialog transactions for loans management, assign the following transactions to it:

- BP
- BCA_DATE_POST_SET
- BCA_DATE_EOD_SET
- BCA_CN_ACCT_01
- BCA_CN_ACCT_02
- BCA_CN_ACCT_03
- CMS_INS_01
- CMS_INS_02
- CMS_INS_03
- BCA_ACC_MST_RUN
- BCA_BL_AL_DISP_SCHED
- BCA_BL_PP_RUN
- BCA_OR_DISB
- BCA_CN_KFG
- BCA_PO_FO_MULTI
- BCA_ACBAL_NEXT_DATE
- BCA_BL_AL_DISP_ITEMS
- BCA_PAYMITEM_CREATE
- /FSPD/ITEM_MAINTAIN
- /FSPD/IPD_MR1
- BCA_PAYMITEM_MAINTN
- BCA_ACBAL_ACC_S
- BCA_ACBAL_ACC_M
- BCA_OR_DFRL
- BCA_OR_RENW
- BCA_GENERIC_MASS_RUN
- BCA_DEH_EVENT_DISPLA
- BCA_ITEM_EX_RUN
- BCA_SL_EX_RUN
- BCA_OR_PAYF
- BCA_OR_TOC
- /FSPD/IPD_MR2
- BCA_OR_TOC_PP_BOTC
- BCA_OR_EU_RESC
- /SAPPO/PPO2

Make sure that the authorization objects mentioned above are included and equipped with full authorization. Here only a template role is presented, which very probably does not fit to your business needs. Note that a role with full authorization for some authorization objects could be highly critical and should be thoroughly checked, if your business requirements are met, before it is used in productive system..

To obtain a role to enable the user to use cross-system functions (technical user), add the authorization objects mentioned above manually to the role created for dialog transactions.

In case of authorization object S_PROGRAM provide full authorization for authorization field P_ACTION and provide the following values for field P_GROUP: /FSPD/PD, FA_01-FA_16, FPC_01-FPC_04, MCM_CSL, MCM_CSLT, PPO_03, UDM_002; F_B05.

6.3 Collateral Management

6.3.1 Authorizations

If a user is to use dialog transactions only, assign the following authorization objects to the user:

Authorization Object	Description
CMS_PCN_02	Authorization for activities (change request mode)
CMS_PCN_01	Authorization for activities (normal mode)
CMS_OMS1	Authorization for all collateral objects other than real estate (replace CMS_OMS from ECC 6.0 onwards
CMS_OMS	Authorization for all collateral objects other than real estate (obsolete from ECC 6.0 onwards)
CMS_CAG	Authorization object for collateral agreements
CMS_RE	Authorization object for real estate objects in CM.
CMS_RBL	Authorization object for receivable in CM.

Characteristic Based Authorizations

In Collateral Management, all the objects must belong to an administration organizational unit. The authorization objects for collateral objects (real estate and other collateral objects) and collateral agreements are based on a combination of the administration organizational unit and the entity type (assigned using a process control key). For receivables, the authorizations are based on the receivable organizational unit, the receivable status and the product. Authorization for receivables is valid only for the receivables created in Collateral Management or even the local copies of the receivables in external credit systems.

You can, for example, use the attribute administration organization unit to differentiate between employee, VIP, and normal customers objects. You can also create objects in these organizational units as characteristics, which can then also be used to protect application data.

6.4 Leasing

For more information, see http://service.sap.com/securityguide → *SAP Business Suite Applications* → *SAP CRM* → *Security Guide for SAP CRM 7.0.*

7 Scenarios using *banking services from SAP*

7.1 Account Origination

The financial service business scenario *Account Origination* is an application for an integrated customer-oriented software solution, linking the front office, SAP CRM Customer Relationship Management (SAP CRM), to the back office (core processing applications for banking or insurance).

The scenario covers the wide variety of processing application flows in the financial services (FS) industry. Sample content is provided for the most requested scenario of origination of loans.

The scenario starts with a customer applying for an FS product that is provided by the FS institute, and ends when the contract is signed by both parties. The scenario includes the analysis of customer data and requirements, the calculation and creation of quotations for the customer, underwriting, risk assessment and validation, as well as parts of the closing and funding process.

7.1.1 Related Security Guides

The recommendations for SAP CRM are also relevant for the scenario *Account Origination*. For more information, see:

Application	Guide
SAP CRM	For more information, see http://service.sap.com/securityguide → *SAP Business Suite Applications* → *SAP CRM*

7.1.2 Authorizations

Account Origination is a cross-system scenario. As such, the linked transactions in the work center of a business profile (CRM WebClient UI) relate to CRM transactions and also to the transactions in the back-end systems. The standard SAP authorization concept should be sufficient for *Account Origination*.

A finance company also provides loans for employees. The origination process includes a scoring or rating request, the results of which are saved in the business partner and the offer. This data must not be visible for other employees because it contains sensitive data, such as collaterals, lending values, loans, and so on. The security of this sensitive data must be ensured. The authorization problem could be resolved if employee loans, and indeed all FS offers for employees, are created using specific business transaction and item types within the CRM business transaction. We recommend that you use a specific customer-defined sales organization to handle employee loans.

Furthermore, the user profile of employees should be restricted in the following authorization objects:

Authorization Object	Description
CRM_ORD_PR	CRM Order – Business Transaction Type
CRM_ORD_OE	CRM Order - Allowed Organizational Units
B_BUPA_GRP	Business Partner – Authorization Groups

To control the maintenance of specific business partner data in FS accounts on the CRM WebClient UI, the user profiles in the authorization object *Business Partner: Authorization Group (B_BUPA_GRP)* should be restricted.

The CRM WebClient UI for FS accounts in SAP CRM is based on the CRM WebClient UI for CRM business partners and therefore offers the same authorization settings; in particular the authorizations for Access Control Engine (ACE) are checked.

7.1.3 User Management

User Types

System	User	Delivered?	Type	Default Password	Detailed Description
CRM system	End user	No	Dialog user	No	Mandatory. User who can access sales and presales transactions. Created by CRM system administrator.
CRM system	XI user	No	System user	No	Mandatory. User for data exchange between CRM and XI system.

You can use SAP components as well as components from other manufacturers as contract and support systems.

The technical implementation of the *Account Origination* scenario requires at least one contract management system for the operational management of the contracts.

7.2 Regulatory Reporting

For information on the authorization concept in Regulatory Reporting, see SAP Note 1385989.

7.3 Apps for Transactional Banking

Several apps are delivered with banking services from SAP 8.0, Support Package 13. These apps allow bank employees to perform tasks, such as the account closure of deposits accounts, with an easy-to-use user interface. Each of the apps comes with template roles that are listed in the following subchapters and that can be copied to own roles and adapted according to a bank's security needs. All of these apps use OData services to communicate with the OData gateway system connected to back-end systems. The gateway and the back-end systems communicate via enterprise web services. The OData services and the web services should be configured to use the HTTPS protocol to ensure secure communication. The technical template role *SAP_FS_TCR_T* (SAP Role for FS - Transactional Apps) is common to all of the apps and is used to define the tiles on the SAP Fiori Launchpad.

7.3.1 Resolve Payment Exceptions

This app allows a bank to manually process the overdrawn accounts of particularly high-value customers. An account is overdrawn if the account balance is below a committed limit, as

defined in the contract between the bank and its customer. The app can be used to handle two use cases: Firstly, when a debit posting causes the account balance to fall below the limit, and secondly when the account balance is already below the commitment limit and a further debit posting is still pending.

The following table contains the template roles delivered for this scenario. They can be copied to own roles and adapted to the specific needs of the bank.

Role	Description
SAP_FS_BCR_CUSTOMERADV	Customer Advisor - Apps
SAP_FS_PCO_POT	PFCG Role for Payment Exception App
SAP_FS_PCO_APP	PFCG Role for Payment Exception App

The app is intended to be used by bank clerks only and not by end users on the Internet. To select work items related to overdrawn accounts and use the app, the *Process Bank Work Item*s app needs to be available in the system landscape.

7.3.2 Resolve Payment Distribution Exceptions

A bank advances a loan to its customer. Under normal circumstances, the customer repays the loan with a predefined frequency and with a fixed amount. The loans management system automatically assigns the repayments (for example, against principal, interest and charges) to the loan account. An overpayment situation occurs when a borrower makes a repayment for an amount that is greater than the loan receivables that are due. This overpayment can be used to pay receivables in advance, for example. This app enables users in the bank's middle office or back office to view, analyze and resolve exceptions that occur due to overpayments.

The following table contains the template roles for this scenario. These roles can be copied and changed to fulfill the bank's specific authorization concept.

Role	Description
SAP_FS_BCR_LOANSPECIALIST_T	Bank Loan Specialist - Apps
SAP_FS_LNS_OVRPYMT_POT	PFCG Role for LWP POT Odata
SAP_FS_LNS_OVRPYMT_APP	SAP FS Loans Overpayment Resolution

The app is intended to be used by bank employees only and not by end users on the Internet. To select work items related to loan accounts with overpayments and use this app, the *Process Bank Work Items* app needs to be available in the system landscape.

7.3.3 Close Deposit Accounts

This app is used to close savings accounts. If an account cannot be closed directly, all the conditions that prevent the closure are displayed and can be resolved. The app is intended to be used by employees in the bank's middle office and not by end users on the Internet. The following table lists all template roles delivered for the *Close Deposit Accounts* app. These roles can be copied to own roles and adapted to the bank's specific needs.

Role	Description
SAP_FS_BCR_MIDOFFICEUSER_T	Middle Office User - Apps
SAP_FS_TOC_POT	PFCG Role for Account Closure App
SAP_FS_TOC_APP	Application Role for Account Closure App

The app can be connected to a document management system where the signature samples for a signature check can be stored. This document management system is chosen by the bank. Therefore, it is the bank's responsibility to ensure that no sensitive or confidential data

is exposed in the communication with the document management system. For example, a bank's employees should not be able to see the signatures of any of the bank's customers that are not assigned to them.

7.3.4 Process Bank Work Items

Process Bank Work Items is a reuseable app that displays a list of requests (for example, posting control orders) that are created in various banking systems. The user can choose a request from this list for further processing.

The following table lists the template roles delivered for this app. These roles can be copied to own roles and adapted to the specific needs of the bank.

Role	Description
SAP_FS_WIM_ITADMINISTRATOR	IT Administrator role for Worklist assignment
SAP_FS_WORKITEM_APP	SAP FS Work Item

The app is intended as a reusable component that is implemented by other apps. *Process Bank Work Items* is used by the *Resolve Payment Exceptions* and *Resolve Payment Distribution Exceptions* apps.

8 Data Protection

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries. This section describes the specific features and functions that SAP provides to support compliance with the relevant legal requirements and data privacy.

This section and any other sections in this Security Guide do not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to additional features that would be required in a particular environment; decisions related to data protection must be made on a case-by-case basis and under consideration of the given system landscape and the applicable legal requirements.

Note that in the majority of cases, compliance with data privacy laws is not a product feature.

SAP software supports data privacy by providing security features and specific data-protection-relevant functions such as functions for the simplified blocking and deletion of personal data.

SAP does not provide legal advice in any form. The definitions and other terms used in this guide are not taken from any given legal source.

Glossary

Term	Definition
Personal data	Information about an identified or identifiable natural person.
Business purpose	A legal, contractual, or in other form justified reason for the processing of **personal data**. The assumption is that any purpose has an end that is usually already defined when the purpose starts.
Blocking	A method of restricting access to data for which the primary **business purpose** has ended.
Deletion	Deletion of **personal data** so that the data is no longer usable.
Retention period	The time period during which data must be available.
End of purpose (EoP)	A method of identifying the point in time for a data set when the processing of **personal data** is no longer required for the primary **business purpose**. After the **EoP** has been reached, the data is **blocked** and can only be accessed by users with special authorization.

Some basic requirements that support data protection are often referred to as technical and organizational measures (TOM). The following topics are related to data protection and require appropriate TOMs:

- **Access control**: Authentication features as described in section *3.2 User Administration and Authentication.*
- **Authorizations**: Authorization concept as described in section *3.3 Authorizations.*
- **Read access logging**: as described in section *8.2 Read Access Logging*.

- **Communication security**: as described in section *3.4 Network and Communication Security*.
- **Availability control** as described in:
  - Section *3.5 Data Storage Security.*
  - SAP NetWeaver *Database Administration* documentation
  - SAP Business Continuity documentation in the SAP NetWeaver Application Help under *Function-Oriented View -> Solution Life Cycle Management -> SAP Business Continuity*
- **Separation by purpose**: Is subject to the organizational model implemented and must be applied as part of the authorization concept.

The extent to which data protection is ensured depends on secure system operation. Network security, security note implementation, adequate logging of system changes, and appropriate usage of the system are the basic technical requirements for compliance with data privacy legislation and other legislation.

Configuration of Data Protection Functions

Certain central functions that support data protection compliance are grouped in Customizing for *Cross-Application Components* under *Data Protection*.

Additional industry-specific, scenario-specific or application-specific configuration might be required.

For information about the application-specific configuration, see the application-specific Customizing in SPRO.

8.1 Deletion of Personal Data

Use

The Transactional Banking component might process personal data that is subject to the data protection laws applicable in specific countries as described in SAP Note 1825544.

The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data. Collateral Management uses SAP ILM to support the deletion of personal data as described in the following sections.SAP delivers a where-used check (WUC) for the Collateral Management system. This is available with SAP Note 2028076 (contains further information about the functionality) and 20022732 (contains the code changes). You implement the WUC in transaction SNOTE.

SAP delivers an end-of-purpose check (EoP) for Business Partner data for the Deposits Management system, and for the Loans Management system. SAP Note 1976105 contains an overview about the functionality as well as a list of all relevant notes which contain the code changes needed for the EoP. SAP Note 2042860 provides information about needed customizing entries to establish the EoP.

All applications register either an EoP in the Customizing settings for the blocking and deletion of the business partner or a WUC. For information about the Customizing of blocking

and deletion for the Collateral Management system, see the section below *Configuration: Simplified Blocking and Deletion*.

End of Purpose Check (EoP)

An end of purpose check determines whether data is still relevant for business activities based on the retention period defined for the data. The retention period of data consists of the following phases:

- **Phase one**: The relevant data is actively used.
- **Phase two**: The relevant data is actively available in the system.
- **Phase three**: The relevant data needs to be retained for other reasons.

  For example, processing of data is no longer required for the primary business purpose, but to comply with legal rules for retention, the data must still be available. In phase three, the relevant data is blocked.

  Blocking of data prevents the business users of SAP applications from displaying and using data that may include personal data and is no longer relevant for business activities.

Blocking of data can impact system behavior in the following ways:

- **Display**: The system does not display blocked data.
- **Change**: It is not possible to change a business object that contains blocked data.
- **Create**: It is not possible to create a business object that contains blocked data.
- **Copy/Follow-Up**: It is not possible to copy a business object or perform follow-up activities for a business object that contains blocked data.
- **Search**: It is not possible to search for blocked data or to search for a business object using blocked data in the search criteria.

It is possible to display blocked data if a user has special authorization; however, it is still not possible to create, change, copy, or perform follow-up activities on blocked data.

For information about the configuration settings required to enable this three-phase based end of purpose check, see *Process Flow* and *Configuration: Simplified Blocking and Deletion*.

Where-Used Check (WUC)

Collateral Management

A where-used check is a simple check to ensure data integrity in case of potential blocking. The WUC in the Collateral Management system checks whether any dependent data for a business partner exists in the following CMS tables:

- CMS_AST_BP
- CMS_SEC_ACC_BP
- CMS_RE_PRT_BP
- CMS_RE_OBJ_PRT
- CMS_CAG_BP
- CMS_CAG_RULES

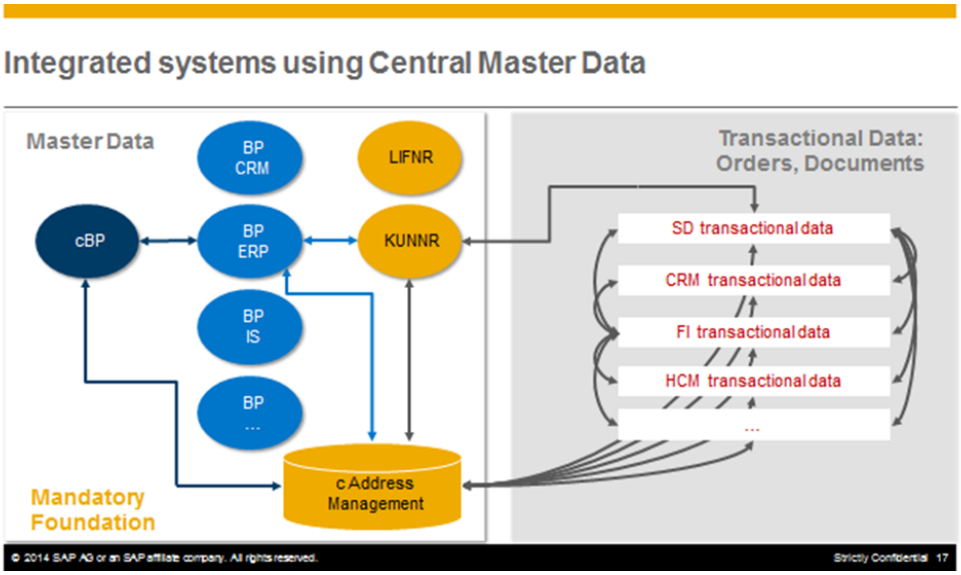
- CMS_RBL_BP

If dependent data exists, that is, if the data is still required for business activities, the system does not block the business partner.

If you still want to block the data, the dependent data must be deleted by using the existing archiving and deletion tools or by using any other customer-specific solution.

Integration with Other Solutions

In the majority of cases, different installed applications run interdependently as shown in following graphic.



Example of interdependent applications

An example of an application that uses central master data is an SAP for Healthcare (IS-H) application that uses the purchase order data stored in Financial Accounting (FI) or Controlling (CO).

Relevant Application Objects and Available Deletion Functionality

Application	*Detailed Description*	*Provided Deletion Functionality*
Financial Services Business Partner – banking services 8.0 from SAP		Archiving object CA_BUPA, *ILM enablement*

Relevant Application Objects and Availability EoP/WUC functionality

Application	*Detailed Description*	*Provided Deletion Functionality*
Collateral Management System – banking services	WUC	WUC checks in tables: • CMS_AST_BP

Application	*Detailed Description*	*Provided Deletion Functionality*
8.0 from SAP		• CMS_SEC_ACC_BP • CMS_RE_PRT_BP • CMS_RE_OBJ_PRT • CMS_CAG_BP • CMS_CAG_RULES • CMS_RBL_BP Customizing views: • V_BUTEOPAPP: CMS application is registered • V_BUTEOPFM: Application-specific WUC function module is registered. WUC: Function module CMS_WUC_BUPA_EOP_CHECK
Financial Services Business Partner – banking services 8.0 from SAP	EOP	EOP Callback function modules for Business Partner and Business Partner Relationships: BUP_BUPA_EOP_CHECK BUB_BUPA_EOP_CHECK
Deposits and Loans Mangament system – banking services 8.0 from SAP	EOP	EOP Call Back Function Module FS_TB_BPDP_EOP_CHECK The dependent objects which needs to be checked in EOP check are organized in check groups. A check group is defined on the basis of data base tables that are relevant to select the existing dependent objects. The SAP standard provides currently 8 check groups. The customer has the possibility to define own check groups additionlally. The order of the checks for check groups can be customize. The following list contains the class in which the EOP check for the relevant check group is implemented: CL_BCA_CONTRACT_BPDP_CHK_EOB (contract check group), CL_BCA_SEPA_CRED_BPDP_CHK_EOB (SEPA mandates check group), CL_BCA_PO_BPDP_CHK_EOB (payment order check group), CL_FS_TB_IM_BPC_BPDP_CHK_EOB (cleansing check group), CL_BCA_CORR_BPDP_CHK_EOB (correspondence check group), /FSCBM/CL_AL_CBM_BPDP_CHK_EOB (checkbook management check group), CL_PRI_BPDP_CHK_EOB (pricing check group), and

Application	*Detailed Description*	*Provided Deletion Functionality*
		CL_BCA_CAH_BPDP_CHK_EOB (account holder change order)

Process Flow

1. Before archiving data, you must define residence time and retention periods in SAP Information Lifecycle Management (ILM).
2. Choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available.
3. Do the following:
    - Run transaction IRMPOL and maintain the required residence and retention policies for the central business partner (ILM object: CA_BUPA).
    - Run transaction BUPA_PRE_EOP to enable the end-of-purpose check function for the central business partner.
4. Business users can request unblocking of blocked data by using the transaction BUP_REQ_UNBLK.
5. If you have the required authorization, you can unblock data by running the transaction BUPA_PRE_EOP.

Configuration: Simplified Blocking and Deletion

You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components* under *Data Protection*.

- Define the settings for authorization management under *Data Protection -> Authorization Management*. For more information, see the Customizing documentation.
- Define the settings for blocking in Customizing for *Cross-Application Components* under *Data Protection -> Blocking and Unblocking -> Business Partner*.

You configure the settings related to the blocking and deletion of customer and vendor master data in Customizing for *Financial Accounting* under *Accounts Receivable and Accounts Payable -> Deletion of Customer and Vendor Master Data.*

8.2 Read Access Logging

Use

If no trace or log is stored that records which business users have accessed data, it is difficult to track the person(s) responsible for any data leaks to the outside world. The *Read Access Logging (RAL)* component can be used to monitor and log read access to data and provide information such as which business users accessed personal data, for example, of a business partner, and in which time frame.

In RAL, you can configure which read-access information to log and under which conditions.

For more information about RAL, see *Read Access Logging (RAL)* in the documentation for SAP NetWeaver.