Application Security Guide for Bank Analyzer Release 4.0

Contents: Depiction of the aspects relevant to the security of Bank Analyzer Release 4.0 (solutions for Basel II and IAS) and description of the required actions		Final	11/03/2004
relevant Bank Analyzer Component	Security	**Authors**	Oliver Kling, Rolf Sieberg

1 Introduction

The Application Security Guide for Bank Analyzer Release 4.0 explains the security-relevant aspects of Bank Analyzer to customers, consultants, support and sales & distribution and describes the actions required to contribute to the secure operation of Bank Analyzer. Prerequisite for understanding the security aspects and actions discussed here is knowing the concepts of Bank Analyzer.

2 General Comments on the Topic of Security in Bank Analyzer

At some points, there are references to related documents, which contain detailed information on topics, which are not covered in this application security guide or for which only an overview is provided. You can access these documents via the SAP Service Market Place (***service.sap.com***). The SAP Service Market Place also offers additional information on security ***service.sap.com/security.***

Basic security aspects and recommended actions are provided in the SAP WebAS Security Guide, which you can access via ***service.sap.com/securityguide***.

 The Application Security Guide for Bank Analyzer Release 4.0 does not substitute studying the SAP WebAS Security Guide but complements its explanations with specifics and additional information in Bank Analyzer. Please read the SAP WebAS Security Guide first and familiarize yourself with the actions described there.

 Use the customer services offered on the subject of security (such as Security Consulting Team, Check list).

The Reporting BW (refer to the definition in the following text) is used as a standard; so please gather all security-relevant information from the documents[1] of the SAP Business Information Warehouse under ***service.sap.com/bw***. The Application Security Guide for Bank Analyzer Release 4.0 does not deal with the Reporting BW.

2.1 Categorization of Security Risks in Bank Analyzer

The data stored in Bank Analyzer is often person-related data subject to data protection acts. Information on transactions, which were made by customers who are also employees of the bank (employee accounts) is particularly distinguished by means of bank-internal agreements.

The data of Bank Analyzer is used to generate balance sheets according to IAS, disclosure reports according to Basel II requirements or incoming data for reporting provider interfaces. The data of Bank Analyzer is thus part of the information, which banks have to disclose.
Furthermore, the results are internally used as the basis for controlling business processes and overall bank controlling. They are thus of strategic value.
The results can then be used to evaluate department or employee achievements (bonus payments, premiums).

[1] When this document was created, there were not yet any application security guidelines for SAP BW.

The following relevant categories of security risks for Bank Analyzer result from the payment notes:

- **Confidentiality/authorization:**
  Unauthorized read access of person-related or strategically relevant information is to be avoided.
- **Integrity:**
  Unauthorized data manipulation with the aim of falsifying the result is to be avoided.

Bank Analyzer evaluated data, which is replicated from operational feeder systems (SAP and non-SAP systems) or which is offered by external providers (such as market data providers). The security of these systems supplying data as well as the data delivery is not the subject of this document.

The description of security measures to avoid unintended loss of data or to reduce the effects of a possible data loss by using suitable data backups are also not discussed in this document.

3 Architecture of Bank Analyzer

The Basel II and IAS solutions, which can be implemented by using Bank Analyzer, use the following architecture:

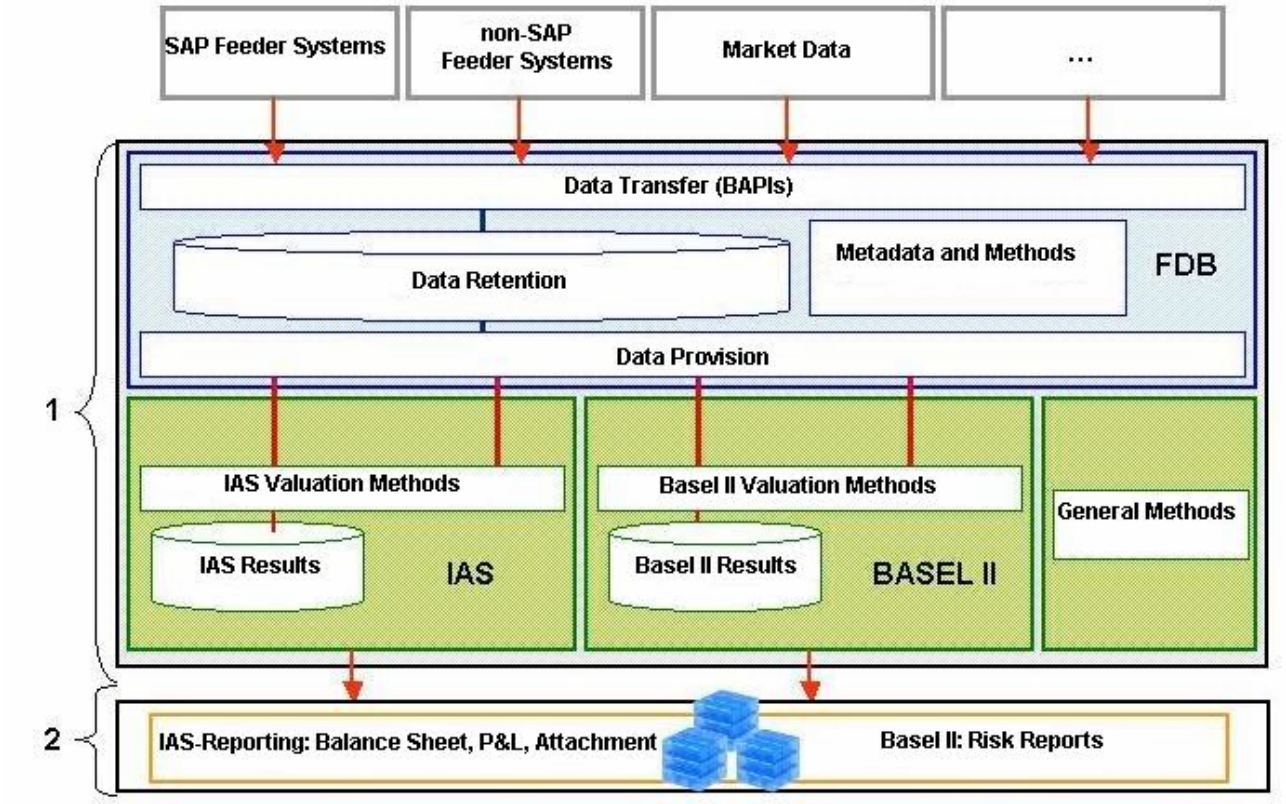

Figure 1: Architecture of Bank Analyzer

This architecture shall be described by using the typical overall processes of these two solutions:

First, the input data from different feeder systems (SAP systems or others) is loaded to the FDB via BAPI interfaces. A transformation process to the consistent data model of Bank Analyzer is required before the FDB can be filled. The FDB stores input information and, in addition to this, offers correction options and business methods such as the generation of cash flows from financial terms.

The analytical valuation procedures of the Basel II and IAS solution can use the communication framework (“Data Provision”) of the FDB to access input data, method results and also results data from other Bank

Analyzer components. The results of further processing of the input information are saved within the corresponding solution by using solution-specific methods.

Apart from the two solutions Basel II and IAS, general methods are available, which can be integrated into the processes of both solutions. If required, the general methods have their own data retention.

The previously described process steps aim to evaluate the FDB input data according to the procedures specified by Basel II or IAS, this means they *produce* results. This part of the solution, marked as “1” in figure 1, is referred to as **Bank Analyzer Core** in the following sections.

The results are not analyzed in the Bank Analyzer Core but in a separate SAP Business Information Warehouse (BW) system, the **Reporting BW**, which is marked as “2” in figure 1. Extractors are offered, which replicate the data into the Reporting BW for further analysis.

The Bank Analyzer Core used a second SAP BW, the **Tool BW** , to be able to provide FDB functions (repository for characteristics and key figures, transactional ODS objects and InfoSets for the FDB index functions). The Tool BW may only be used for these functions. Due to the very restricted use of the Tool BW, it is possible to take security measures in this system, which are more restrictive than those specified in the SAP BW documentation.

The following authorization objects are to be defined:

If the user is only to be able to carry out application functions you should use the following authorization objects (only one reading activity each - 03, sub-objects DATA and DEFINITION):

- Authorization object S_RS_ODSO (Get Details of ODS-Object, Get Data in ODS-Object)
- Authorization object S_RS_ISET(Get Details of InfoSet, Get List of InfoSets, Get InfoSetData, Get InfoSetData in Package)

If the user is to carry out the FDB configuration, the following authorization objects are to be used:


Table_01.xls

4 Network Security and Communication

The network infrastructure is very important for the security of the system. With regards to the communication channels Bank Analyzer basically functions as described in the SAP WebAS Security Guide. It thus does not offer any customer-developed communication channels or similar. Hence the aspects and actions described in the SAP WebAS Security Guide (such as use of SAPRouter in combination with Firewall, use of Secure Network Communication (SNC), Communication Front-End-Application Server, connection to the database) also apply for Bank Analyzer.

The data flows relevant to the operation of Bank Analyzer are depicted in the following graphic:

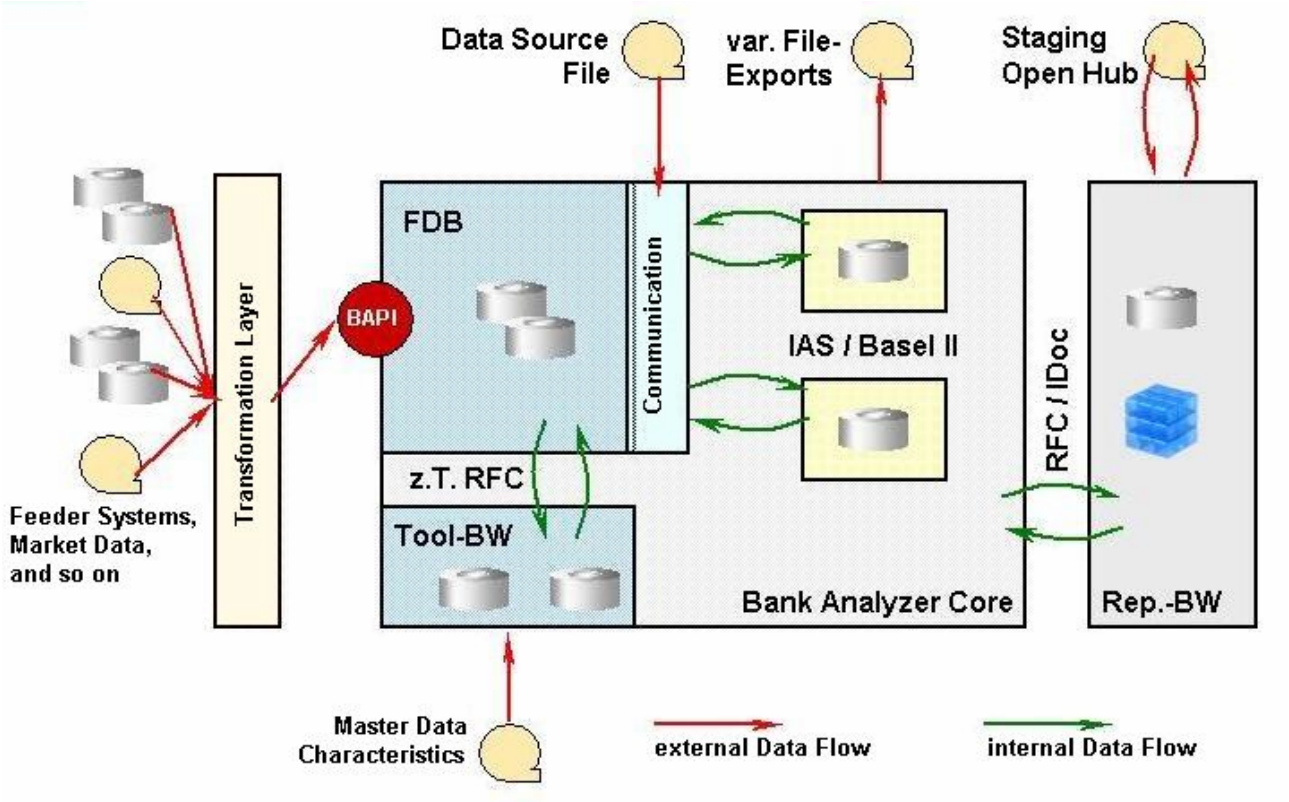

Figure 2: Data flows in Bank Analyzer

In the following sections, we differentiate between internal and external data flows.

4.1 Internal Data Flows

In figure 2, internal data flows are green; they are distinguished by the fact that the source and target of the data flow are Bank Analyzer components.

In turn, internal data flows can be split into local data flows, which do not cross any system boundaries, and non-local data flows.

- local data flows:
  Communication of Bank Analyzer Components by calling function modules or methods (such as the communication framework (primary data sources) of the FDB).
  No special security measures in addition to the SAP WebAS Security Guide are required with regards to the security of these internal local calls.
- non-local data flows:
  Communication with a BW system (Tool BW or Reporting BW). This communication happens via RFC or during data extraction by means of extractors also via IDOCs. The communication is secured via SAP's Secure Network Communication (SNC) concept, whereby the following restriction has to be kept in mind:

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


SAP does not ship any RFC connections. Please pay attention to the notes in the SAP WebAS Security Guide when setting up internal non-local data flows.

However, the following RFC connections have to be set up to operate Bank Analyzer. Do not create the users belonging to these as dialog users.

- RFC communication with the Tool BW: see chapter [3]
- RFC communication within the Tool BW (RFC call in the BW standard client): 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, S_RS_ISET

4.2 External Data Flows

In figure 2, external data flows are read. They are data flows for which either the source or the target is not a Bank Analyzer component.

Bank Analyzer knows the following interfaces:

- BAPI:
  The supply of data from the operational feeder systems or other external providers to the FDB, Tool BW and HDB happens via BAPIs.
  The list of BAPIs can be retrieved with the transaction “BAPI”. Here you will also find documentation referring to corresponding authorization objects.
  Some BAPIs will be called from Bank Analyzer processes, e.g. the FDB-BAPI for the creation of stress test scenario data will be called by the HDB. In this case, BAPIs play a role in internal data flows as well

  The BAPIs of the FDB carry out the same authorization checks as the manual processing of objects. Note the following exception: The “complex authorization check” is not carried out for automatic data imports.

- File:
  Files can be used as follows:
  - Input:
    - The FDB gives every Bank Analyzer Core component access to external files via the communication framework (primary data source).
    - The SAP BW offers the option of importing files.
      You can use this option in the Tool BW to load master data, meaning texts, attributes and hierarchies for characteristics.
      You can use this option in the Reporting BW to load master or transactions data to supplement extracted Bank Analyzer Data.
    - The DX Workbench offers the option of importing files and calling BAPIs.
    - In systems which are not used productively, you can import Excel files with test data for accounting. The procedure is additionally secured via authorizations. Please use the options offered by the FDB and not the interface.
    - The Historical Data Base HDB offers a GUI-Upload, by means of which text or XML files may be loaded into data collection area of the HDB.
  - Output:
    - The Bank Analyzer Core offers operational reporting based on ABAP List Viewer (ALV) lists. A download function is offered for already displayed data.

- The Bank Analyzer Core offers different processes (such as FDB data export, interface to reporting) whose aim is or can be to export data to files.
- If Bank Analyzer Data can be archived, the standard tool ADK (Archive Development Kit) is used. The data to be archived is usually written to files.
- With the open hub interface, the SAP BW offers the option of extracting data which is saved in the BW to files.
- Reports, which were generated in the SAP BW, can be downloaded to file with the means of the front end used (MS Excel, internet browser).
- In the context of the HDB run, Bank Analyzer data can be transferred to bank-internal models via an outbound BAPI (refer to the documentation for the InputWrite method if the InternalModelHDB business object as well as documentation for BADI /BA1/R6_INTERNAL_MDL). The concrete configuration of the transfer (and thus the inclusion of possible confirmation prompts) is made in the context of implementing the BADI and is thus customer-specific (see section 8.2).
- The Historical Data Base HDB offers a GUI-Upload, by means of which Bank Analyzer data may be exported into text or XML files. The selection of data (from FDB, HDB or other Analyzers) as well as manipulation of the selected data in main memory before the output is done in the data collection area of the HDB.

 The fact that all files are not within the scope of the SAP protection options (authorizations…) applies to all these options. The customer alone is thus responsible for the security of the files and the confidential data in these files.

The Basis authorization object S_DATASET exists for access to files from the SAP back-end. You should restrict authorizations for this object.

- The data staging function of the SAP BW can be used for the Tool BW and the Reporting BW according to the requirements of the BW.

   Here, Bank Analyzer does not guarantee the data quality and the security of the data sources; the customer has to deal with these separately.

4.3 Additional Communication Channels

In addition, it is also possible to display or call up reports and other transactions in the SAP Enterprise Portal.

 The SAP Enterprise Portal is to be secured according to the standard.

5 Security of the Data Backup

The Bank Analyzer data is secured in the system data basis. This does not differ from the SAP WebAS Security Guide.

There are not additional places, where data can be saved temporarily. You have to differentiate between Customizing and application data:

- Customizing data is typically generated, changed and possibly deleted manually during implementation and sometimes while the system is in operation. In some areas automatic delivery is also possible.
  If the components of the Bank Analyzer Core offer deletion reports, these are protected via the authorization concept or check whether the system is flagged as a production system. In this case the program is not executed.

- Application data is typically loaded to the FDB automatically when the system is in operation and processed further automatically. Manual processing functions of the FDB, which are to be protected by authorization issue, are offered. The FBD manages versions of each change via a technical timeframe. In addition to that corrections can be recorded by the correction server. The components of the Bank Analyzer Core, which follow the FDB, deal with the saving of the process results individually. Depending on the solution, posting, correction, reversal, deletion and archiving functions are offered for the saved results data. These functions have to be protected via the authorization concept. For more detailed information, refer to the documentation of these components.

   The IAS solution includes the report /BA1/RB1_TT_DELETE_APP_DAT, which can delete selected application data. This report cannot be executed in the production systems.

The delivered software does not have any default parameters, which expressly protect Customizing data or application data already. The level of protection required has to be ensured via the issue of authorizations as well as system settings (such as the changeability of clients).

6 User Interface

The Bank Analyzer Core uses the standard SAP GUI. Use via the Internet Transaction Server is not supported.

Depending on the implementation of reporting, the use of the Reporting BW can also be used with an Internet browser as the user interface (SAP Internet Transaction Server – WebAS-Security).

7 User Administration and Authentication

Technical users and dialog users are used in Bank Analyzer. No users are shipped apart from the standard users described in the SAP WebAS Security Guide. All users are created by customer-specific system administration, which also provides the initial identification parameters (such as password).

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

7.1 Authorizations

7.1.1 Roles

A multitude of roles and composite roles are already shipped with Bank Analyzer Release 4.0. These roles are of exemplary character. They are to be adjusted by the customer and are not to be used in the shipped form in production systems.

You can find the available roles by using the transactions PFCG (Profile Generator) in the system.

You can use the Profile Generator to create additional roles.

7.1.2 Characteristic-Based Authorizations

Bank Analyzer works with freely definable characteristics. In all components of the Bank Analyzer, it is necessary to make certain authorizations dependent on the values of individual characteristics. This also applies to customer-specific characteristics.

Bank Analyzer is thus designed for a variable assignment of (customer-specific) characteristic to the fields of the predefined authorization objects. The assignment happens by means of dedicated customer Customizing. For more detailed information please refer to the SAP Library in Bank Analyzer.

 Use this option, for example, to particularly flag and protect employee accounts with a characteristic. You can also create organizational units as characteristics, which can then also be used to protect Customizing and/or application data.

7.1.3 Particularities regarding the Drill-Through of the Reporting BW

The registration in the Bank Analyzer Core system is required because of the drill-through via the report-report interface (refer to the SAP Library of the BW) from reports of the Reporting BW into the Bank Analyzer Core. Please note that authorizations in the Reporting BW can be issues independently of the authorizations of the Bank Analyzer Core.

 Be consistent when issuing authorizations in the Reporting BW and in the Bank Analyzer Core. In doing so, you avoid enabling access to data in one system, while disabling access to another system.

You should thus co-ordinate the authorizations for the targets in the Bank Analyzer Core with those in the Reporting BW.

8 Other Security-Related Notes

8.1 Use of the SAP Development Environment

At this point we would like to point out that authorizations for the SAP development environment should only be issued very restrictively. Users with the development or debugging authorization who are also authorized to change the field contents in the debugger, can potentially read, change or delete any information in Bank Analyzer. (They can, for example change information by calling the relevant BAPI and avoiding the programmed authorization checks for the planned use.) These users can also modify system parameters. Please refer to the SAP WebAS Security Guide for information on how to avoid access to the SAP development environment.

 Be very restrictive when issuing development authorizations. Ensure organizationally (principle of double control, code reviews) that no code gets into the system without being checked first. A simple test of the code-containing Customizing in the test system is **not** sufficient, as it is possible to let the harmful code sequences only run in the production system.

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

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

The tools of Bank Analyzer (such as the derivation tool, Module Editor…) can be used to access function modules. It is possible to include user-defined function modules according to the application.

 All options of the ABAP workbench are thus available in both cases. This means that (undocumented) read or change access to any information in Bank Analyzer and many system parameters is potentially possible. Generally, SAP does not guarantee the security of non-SAP

implementations/enhancements/modifications at this point. SAP cannot provide technical protection against this type of abuse.

8.2.1 Messaging Application Programming Interfaces in the Area of Accounting

IAS accounting provides the following MAPIs for connecting an external hedge management system:

- Already available with release 3.0/3.1
  - /BA1/B1_MAP_HTB_DEDESIGNATION
  - /BA1/B1_MAP_HTB_DESIGNATION
  - /BA1/B1_MAP_HTB_DISSOLUTION
  - /BA1/B1_MAP_BTA_DOCUMENTS_SAVE
  - /BA1/B1_MAP_BTA_INTERNAL_SET
  - /BA1/B1_MAP_BTA_REF_STRUCT_GET
  - /BA1/B1_MAP_BTA_REVERSAL_SET
  - /BA1/B1_MAP_US_UPDATE_HEDGE
- new with release 4.0
  - /BA1/B1_MAP_FP_GET_DESC
  - /BA1/B1_MAP_FP_GET_PARTICIPANT
  - /BA1/B1_MAP_FP_GET_STATUS

These MAPIs are not protected by special authorizations.

However, a “remote” call of these MAPIs is not possible.

8.3 The Step Types *Formula* and *Condition* in the Module Editor

The Module Editor interprets the Customizing that was entered and uses it to generate code. You can enter any number of ABAP statements in the step types *formula* and *condition*, as long as each statement finished with a full stop. In doing so, all options of the ABAP workbench are available (see chapter [8.1]).

 Such a use of the listed step types of the module editor has ***not*** been Released by SAP.

 No development authorization is required to make Customizing settings in the module editor. The coding sequence, which was created as described, can also be created by users who only have Customizing authorizations.

 The module editor offers a test function. This function facilitates the testing of modules, which haven’t been activated. It is thus conceivable to create, execute and remove coding sequences as described. Because this leaves all possibilities of the ABAP Workbench open, 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. In this context you should also pay attention to SAP Note 676390, which deals with the topics of Customizing and transport in the environment of the module editor.

 Ensure organizationally (principle of double control, code reviews) that no module gets into the production system without being checked first. A simple test of the Customizing in the test system is **not** sufficient, as it is possible to let the harmful code sequences only run in the production system.

8.4 Data Aggregation Processes in the Historical Database/Descriptive Statistics

Data aggregation processes are used in the Historical Database. 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 if a user has no authorization for displaying data records for certain characteristics (called Category A characteristics in this text), if these data records contain particular characteristic values for which he or she has no authorization. These constraints do not apply to other characteristics (Category B characteristics).

 If this user then starts data aggregation, and the results of aggregation are only non-initial characteristic values for Category B characteristics, then 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.

> Example: 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, for example, of business partner *BP1*.

9 Security of Additional Applications

No additional applications are required to operate Bank Analyzer.

If other SAP applications, which are not explicitly mentioned in this document, are to be used (such as Collateral Management System (CMS), SEM Business Planning and Simulation), then their individual security guides apply, which have to be considered in a cross-application security concept.