



EASY SOFTWARE AG
Report
Audit of the archive system

Report

Audit of the archive system
EASY ENTERPRISE.x
Version 2.0 SR1

EASY SOFTWARE AG
Mülheim an der Ruhr, Germany

Contents

1	Assignment and performance of assignment	1
1.1	Subject of audit.....	1
1.2	Nature and extent of the audit activities	1
1.3	Basis of assessment	2
1.4	Engagement Terms	3
1.5	Restriction of use.....	3
2	Summary of audit results and software certificate	4
3	Audit results in detail	6
3.1	System overview	6
3.1.1	Archiving functions.....	6
3.1.2	Technical components.....	7
3.1.3	The test environment used.....	8
3.2	Audit of processing functions.....	10
3.2.1	Capturing and quality checks	10
3.2.2	Archive storage	11
3.2.3	Indexing and querying (Retrieval)	14
3.2.4	Reproduction	16
3.3	Validating software security	17
3.3.1	Access protection	17
3.3.2	Data backup and recovery procedures	18
3.3.3	Program development, maintenance and release	19
3.3.4	System communication and logging (Audit Trail).....	20
3.4	Procedural documentation	21

Attachment index

General Engagement Terms	1
---------------------------------------	----------

1 Assignment and performance of assignment

1.1 Subject of audit

With letter of December 7, 2005 and an additional letter of February 15, 2006, we were appointed by

EASY SOFTWARE AG of Mülheim an der Ruhr, Germany,
-- referred to in the following as "EASY" or "Company" --

to carry out a regulatory audit on the following software developed and sold by EASY:

"EASY ENTERPRISE.x" and other additional components
-- referred to in the following as "EE.x" --

1.2 Nature and extent of the audit activities

As agreed with EASY, our audit of the EE.x software included the following modules and components:

- EASY ENTERPRISE.x Version 2.0 SR1
(core functions for archiving, management as well as database- and full text-based retrieval of documents)
- EASY DOCUMENTS Version 3.51
(additional component for document-based electronic processing)
- EASY WORKFLOW Version 1.2
(additional component for rules-based workflows)
- EASY COLD Version 3.50
(additional component for fully automatic archiving of outgoing print documents)
- EASY CAPTURE Version 3.50
(scan product for paper-based capturing of bulk data)
- EASY for mySAP Version 2.0 SR1
(interface to Archive Server and SAP)
- EASY xBASE Version 3.50
(interface to Microsoft Exchange for archiving e-mails)
- EASY NOTES Version 2.0 SR1
(interface to Lotus Notes for archiving e-mails)

The purpose of this audit was to find out whether the software allows the capturing, indexing, storing, querying and retrieval of documents in compliance with the commercial and tax law regulations.

The current EE.x version and the additional components listed above were the subjects of our audit. Our audit does not cover follow-up versions of the Software or risks that may arise from legal changes after our audit has been completed.

The following issues were not included in this audit:

- Assessing requirements for deploying hardware and IT infrastructure.

Our tasks were performed by reviewing the given documentation, by interviews with employees of EASY SOFTWARE AG as well as system based audit procedures during the period from January 23 to February 25, 2006 in the company's premises in Mülheim an der Ruhr, Germany.

Type and scope of our analysis are documented in our working papers.

1.3 Basis of assessment

The following regulations and professional standards are the basis of our audit:

- IDW auditing standard "Issue and Use of Software Certifications" (IDW PS 880), version June 25, 1999;
- The legal requirements of commercial and fiscal law, in particular Sections 238 to 257 German Commercial Code (Handelsgesetzbuch, HGB) and Sections 145 to 147 German Fiscal Code (Abgabenordnung, AO) as well as,
- Generally Accepted Accounting Principles in Computer-Assisted Accounting Systems, GAPCAS (Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme, GoBS), as published in the Federal Fiscal Gazette (Bundessteuerblatt) 1995, Part 1, No. 18, P. 739 ff.,
- The Basic Regulations for Accessing Data and Auditing Digital Documents (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen - GDPdU) as published by the German Federal Department of Finance on July 16, 2001
- The provisions of the German Federal Data Protection Law (Bundesdatenschutzgesetz - BDSG);
- IDW Audit Standard: Audit of financial statements using information technology (IDW PS 330) as well as,
- IDW statement concerning accounting: Principles of Proper Accounting for the Use of Information Technology (IDW RS FAIT 1),

1.4 Engagement Terms

The General Engagement Terms for auditors and audit firms as of January 1, 2002 (see appendix) are applicable for the duration of the assignment. Maximum liability is determined in accordance with point no. 9 of the General Engagement Terms and the supplementary written agreements. No. 1 (2) and no. 9 of the General Engagement Terms are applicable with regard to relations between third parties.

1.5 Restriction of use

EASY SOFTWARE AG agreed to dispense with any statement of the audit results on references to submitting a testate to IDW PS 880, e.g. on the company's website. For more information users must be referred to the audit report, which will be available online on the servers of KPMG after accepting the General Engagement Terms for auditors and auditing companies in the version of January 1, 2002.

2 Summary of audit results and software certificate

The commercial and tax provisions basically allow retention of accounting related documents on digitized storage media (see Clause 239, Paragraph 4 HGB (German Commercial Code), Clause 147, Paragraph AO; GoBS). From a technical point of view, a distinction must be made between “Coded information (CI)” and “Non coded information (NCI)” types.

EASY ENTERPRISE.x is a document management system used for capturing, storing and reproducing documents in data archives that are, amongst others, used for retention of accounting related information. The software must meet the requirements of the Commercial Code and the Fiscal Code, insofar as

- documents subject to retention are archived using the software, and
- digitally stored documents fulfil the accounting records, journals and accounts functions.

The EASY ENTERPRISE.x Version 2.0 SR1 (build 1319.evo14) software as well as the in the audit scope defined components which were the subject of our audit, ensure proper transformation of information subject to retention. If properly used, the software enables capturing, indexing, storing, querying and reproducing electronic documents in compliance with the German Principles of Proper Accounting. The defined system settings ensure secure, permanent and revision-proof archiving of documents in compliance with the German Principles of Proper Accounting on deploying information technology.

In addition, the audited software product, when applied accordingly meets the requirements of the German Department of Finance (Bundesministerium für Finanzen – BMF) of July 16, 2001 regarding the Basic Regulations for Accessing Data and Auditing Digital Documents (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen – GDPdU). It is imperative that the respective user accomplishes the required organizational and procedural requirements for complying with GDPdU requirements, such as defining tax related and original digitized data as well as data extraction from data systems, ensuring machine-aided and GDPdU-compliant analyzability of relevant data assets.

Within the scope of checking the functions we established that CI and NCI documents are properly stored in a data archive, that they match the original documents in terms of images and data, that they are available for the duration of the retention period, and that they can be instantly made readable at any time.

The underlying procedural documentation is up to date and traceable.

The following measures must be ensured and performed for proper software operation by the respective user:

- Proper allocation of user and administration authorizations must be ensured.
- Unchangeability of archived documents must be ensured over the entire period of retention. For this purpose, the functions provided by the application can be used.
- A suitable data backup concept for additional components and the archive system's data assets must be included in the user's consideration for protection against loss of data in case of a disaster.
- To ensure that legal regulations on the retention of data are met, an appropriate enterprise-specific archiving concept must be created.
- After destroying the original document, the opto-electronically archived document will be valid as the document of the respective business transaction. Organizational provisions must be made accordingly.

Our results, assessments and recommendations are described in detail in Chapter 3.

Cologne/Germany, March 2, 2006

KPMG Deutsche Treuhand-Gesellschaft
Aktiengesellschaft
Auditing company



Geesmann
Partner



ppa.
Tenkhoff
Senior Manager

3 Audit results in detail

3.1 System overview

3.1.1 Archiving functions

EASY ENTERPRISE.x is a software product used for revision-proof archiving of documents. The system supports scan, create, index, archive, query and search documents functions. In addition to scanned documents (Non-Coded Information – NCI), any files (Coded Information – CI), e.g. from text processing, spreadsheet calculation, image processing, e-mail or ERP systems are considered as documents.

On the system side, documents are saved in electronic archives, i.e. pools. Archived documents are accessed via client applications (EASYiDOX, EASYiDOX WEB) by analyzing index information saved in a separate database.

The products EASY CAPTURE and EASY COLD are additional components for capturing documents. While EASY CAPTURE is a scan product for paper-based capturing of bulk data, EASY COLD is used for archiving and indexing electronically created print documents automatically.

The products EASY DOCUMENTS and EASY WORKFLOW, which are also included in this audit, include functions for electronic document management, defining and handling rule-based document workflows as well as integrating them into the EASY ENTERPRISE.x archive system.

The EASY xBASE and EASY NOTES components are used to link the Microsoft Exchange or Lotus Notes e-mail systems to the EASY ENTERPRISE.x archive system for manual or automatic archiving, search/retrieval and restoration of e-mail documents and their attachments.

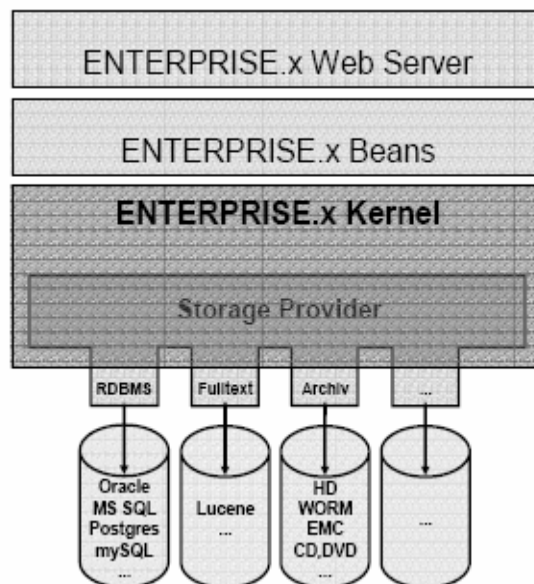
Linkage to the standard ERP system SAP R/3 is supported by the EASY for mySAP product suite, which consists of the products Level 1, Level 2, SmartLink and SAP Retrieval.

The Level 1 interface includes functions for storing, searching and reproducing documents (delivery notes, invoices, etc.), print lists or SAP R/3 document data in compliance with SAP ArchiveLink standard. This standard interface was certified by SAP AG, Walldorf, Germany. Assessing that certification was not within the scope of this audit. The products Level 2 and SmartLink extend SAP R/3 linkage with functions for automatically linking archive documents with business objects within the SAP R/3 systems as well as for automatically indexing archive documents using detailed SAP R/3 system information. The product SAP Retrieval is used to integrate retrieval functions with SAP GUI enabling retrieval and display of archived documents within an SAP R/3 environment.

3.1.2 Technical components

On the server side, the EASY ENTERPRISE.x archive system consists of at least one archive server that requires a J2EE (Java 2 Enterprise Edition) application server and a Web server as the runtime environment. Additionally, a relational database accessed via JDBC, and a full text database is required for saving index and configuration tables. The "Lucene" Open Source full text database is part of the EASY ENTERPRISE.x Archive server package. It is automatically installed along with the standard installation.

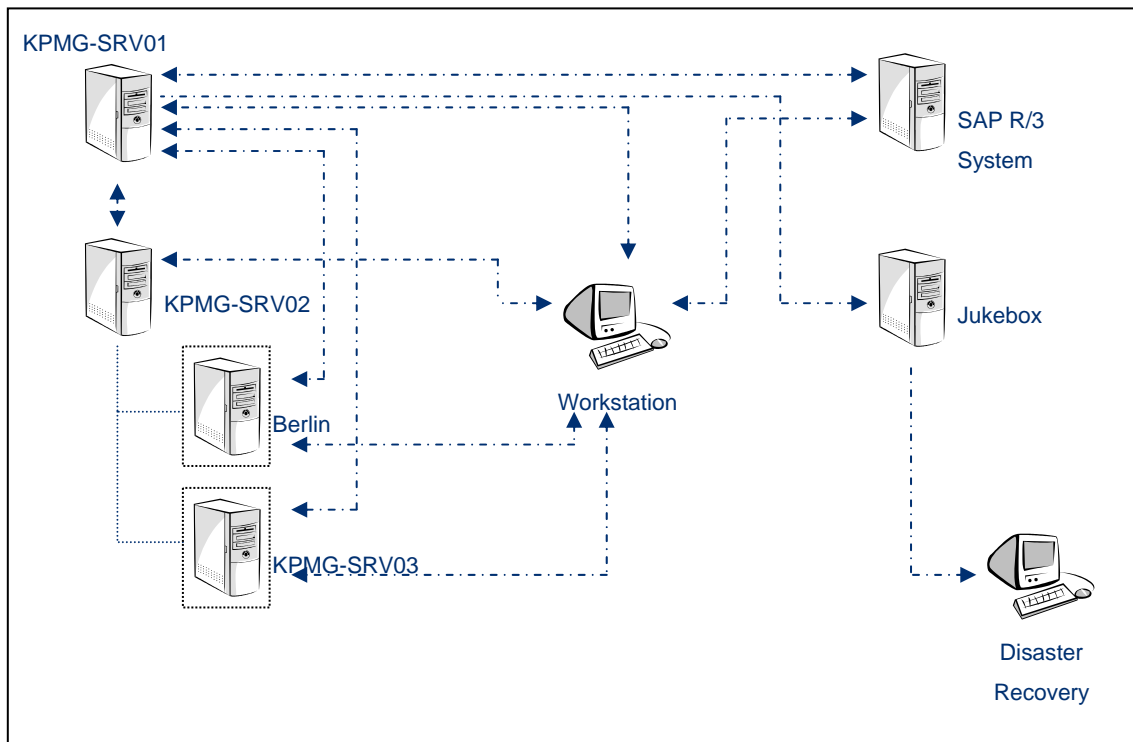
Below is a schematic diagram that shows the EASY ENTERPRISE.x Archive server's architecture:



Users can access the archive solution through the client applications (EASYiDOX, EASYiDOX WEB) which come with the package. Additionally, the application provides its functions via an XML interface. This enables customized access to the system from customers' programs.

3.1.3 The test environment used

For the period of inspection, the Group provided the following test environment on which our inspection results are based:



The table below contains a list of hardware and software components provided in the context of our audit.

Server label	KPMG-SRV01
Function description	EASY ENTERPRISE.x Archive Server and platform for additional components
Hardware description	Dell PowerEdge 2850 Intel Dual Xeon 3.8 GHz 4 GB memory LSI Logic 53C1030 Ultra 320 SCSI onboard 4 hard disks at 140 GB each (total: 560 GB) storage capacity Optical Jukebox Plasmon M20, 1 optical drive, 3 disks at 2.6 GB storage capacity each
Software components	Microsoft Windows Server 2003 Enterprise operating system German SP1 EASY ENTERPRISE.x 2.0 SR1 (build 1319.evo14) SUN Java SDK 1.4.2 JBoss 3.2.7 EASY NOTES Version 2.0 SR1 EASY for mySAP Version 2.0 SR1 EASY LOGISTICS CENTER (EASY DOCUMENTS) Version 3.51

Server label		KPMG-SRV02
	Function description	Database server and host for two virtual servers
	Hardware description	Dell PowerEdge 2850 Intel Dual Xeon 3.8 GHz 2 GB memory LSI Logic 53C1030 Ultra 320 SCSI onboard 3 hard disks at 140 GB each (total: 420 GB) storage capacity
	Software components	Microsoft Windows Server 2003 Enterprise operating system German SP1 Microsoft SQL Server 2000 Service Pack 4 EASY xBASE 3.50 Microsoft Virtual Server 2005 VMware Workstation 4.5.2
Server label		Berlin (virtual server on host KPMG SRV02)
	Function description	Domain Controller and Microsoft Exchange Server
	Hardware description	Dell PowerEdge 2850 Intel Dual Xeon 3.8 GHz 512 MB memory 16 GB virtual hard disk storage capacity
	Software components	Microsoft Windows Server 2003 Enterprise operating system German SP1 Microsoft SQL Server 2000 Service Pack 4 Microsoft Exchange Server 2003
Server label		KPMG-SRV03 (virtual server on host KPMG SRV02)
	Function description	Lotus Domino Server
	Hardware description	Dell PowerEdge 2850 Intel Dual Xeon 3.8 GHz 512 MB memory 60 GB virtual hard disk storage capacity
	Software components	Microsoft Windows Server 2003 Standard operating system English SP1 Lotus Domino Server 6.5.4
Server label		SAPD47
	Function description	SAP R/3 database and application server
	Hardware description	Dell Server Powerededge P2600 Intel Dual Xeon 2.4 GHz 2 GB memory DELL PERC 4/Di RAID-Controller 136 GB hard disk space; Raid 1 consisting of 2 hard disks
	Software components	Microsoft Windows 2000 Server operating system SP4 SAP R/3-Release 4.7, Extension-Set 2.00 – Kernel 620 Patch Level 1732 Oracle 9.2.0.4.0

Server label		KPMG-SRV04
	Function description	Disaster Recovery Server
	Hardware description	Dell OptiPlex 520GX Intel Pentium 4 3.2 GHz 2 GB memory Adaptec 2940AU SCSI Controller 140 GB hard disk space
	Software components	Microsoft Windows Server 2003 Enterprise operating system German SP1 EASY ENTERPRISE.x Version 2.0 SR1 (build 1319.evo15) EASYiDOX 1.0 SUN Java SDK 1.4.2 JBoss 3.2.7 Microsoft SQL Server 200 Service Pack 4
Server label		KPMG client
	Function description	Client for performing function tests
	Hardware description	Dell OptiPlex 520GX Intel Pentium 4 3.2 GHz 2 GB memory FireWire Controller 140 GB hard disk space Kodak i160 Scanner
	Software components	Microsoft Windows XP operating system SP2 EASYiDOX 1.0 EE.x 2.0 SR1 COMMON OPTIONS (build 1577) SUN Java SDK 1.4.2 Microsoft Office u. Visio 2003 Service Pack 2 Lotus Notes Client Version 6.5

3.2 Audit of processing functions

3.2.1 Capturing and quality checks

Requirement:

The archiving system must provide options to scan hard copy documents (NCI) at the quality level required for revision-proof storage, thereby preventing information contained in the original document from getting lost. Capturing quality checks should be possible. On the system side, function separation between scanning and quality checks should also be possible and replicable in the authorizations concept.

Findings:

We ascertained that the application meets the above requirements in terms of the quality of scanned documents.

While the client software modules EASYiDOX and EASYiDOX WEB are available for scanning single hard copy documents, bulk capturing is performed using the software product EASY CAPTURE. The quality of scanned documents is neither restricted by the EASY ENTERPRISE.x system nor by the client software used, but only by the performance of the scanner used as well as its driver software. This basically allows scanning at any resolution in black & white, greyscale and colour, customizing contrast and brightness as well as scanning document flip sides. EASY CAPTURE also provides functions for recognizing empty pages by defining threshold values regarding document size.

In the context of these function tests, hard copies were scanned both in colour and in black & white, at a resolution of 300dpi.

By default, scanned images are displayed on the screen directly after scanning where visual quality checks can be performed. The functions for inverting and the option to rotate the scanned images in 90° increments are available.

To enable segregation of duty between scan workstation and quality checks, the scanning and indexing steps can be performed by various users when using the client software EASY CAPTURE. This separation of functions can be replicated on the system side by setting up authorisations in the EASY CAPTURE configuration. The EASYiDOX and EASYiDOX WEB clients do not allow such immediate function separation. When using so called live documents and properly allocated user authorizations, however, segregation of duty can also be implemented within the EASYiDOX and EASYiDOX WEB clients.

3.2.2 Archive storage

Requirement: Completeness of storage

The process of digital storage must be designed in such a manner that all documents are archived completely and in a sequence organized in factual and/or chronological order.

Findings:

Our audit submitted that the application meets the requirements for completeness of document storage.

The client software or additional components EASYiDOX, EASYiDOX WEB, EASY xBASE, EASY NOTES, EASY DOCUMENTS or EASY WORKFLOW as well as EASY for mySAP ensure complete archiving by using transactions for saving each individual document. Transactions are completed successfully only if the EE.x archive server correctly stored both document data (BLOBs) and index information. Errors occurring during the archiving process are logged on the system side, and need to be processed manually (e.g. EASYiDOX) or automatically (e.g. EASY xBASE) depending on the application used by an attempt of re-archiving the respective document.

EASY CAPTURE and EASY COLD, the software products designated for bulk capturing, use the “Spooler import” function. During the capturing process, documents are initially stored locally on the client in a specific import format. Following this, the documents contained in the export file are transferred to the archive server using the “Spooler Import” program. While they are transferred the documents are initially saved in an import queue. If the documents cannot be archived due to a technical error, the documents will not be lost even if you shut down the archiving server. The documents saved in the import queue can be properly processed after fixing the technical error and restarting the archive server.

Requirement: Unchangeability of documents

For application scenarios where legal requirements or internal corporate guidelines stipulate the use of unchangeable media, the application should support the use of such media. The documents should be archived in a structure preventing changes by users or administrators. In addition, the period during which documents reside on rewritable cache memory prior to transfer to an unchangeable medium should be controllable through parameters dependent on time and size.

Findings:

Our audit submitted that the application meets the requirements for the unchangeability of documents during storage.

On the system side, the documents are initially saved on hard disks in compiled structures of description and content data, i.e. data containers. Although in principle users or administrators might be able to manipulate the documents stored in the data containers, manipulation without far-reaching knowledge regarding the internal structure of the container files is largely precluded.

If the containers are saved permanently on hard disks, the user should take effective measures in terms of container file security, such as restrictive guidelines for network authorizations, the use of data encryptions at operating system level and, if necessary, segregation of duty between network and archive administration.

The application supports the use of different storage systems such as WORM disks. Sealed data containers must be manually transferred to the respectively linked storage system by using the Configuration Manager or a batch program. The size of the respective container files and the time up to possible transfer can be limited through the corresponding system configurations. In addition, the option to seal individual data containers manually using the Configuration Manager to enable premature transfer is available.

The complete and correct transfer of data containers to the storage system media is automatically ensured on the system side by hash sum comparisons of the files. Only on successful hash sum verification the transferred data containers on the archive server will be replaced with a link to the data saved on the archive medium.

Requirement: Traceability of document storage

To guarantee traceability of the archiving procedure, the application should provide an option to find out which user has archived each document and at what time. Changes to archived documents must be traceable. The original version must still be recognizable after the change.

Findings:

Our audit submitted that the application ensures traceability for document storage when configured properly.

For each archived document, the user name of the creating user and the time of archiving are saved as system attributes. These system attributes are mandatory fields which each document schema contains by default. Changes to the contents of the named fields by users are not possible.

When a document is altered, the original document, subject to the document schema configuration, will not be overwritten instead a so-called version is created. That version is a new document whereby the changes and a link to the original document are saved. In this way a document history is possible whereby the original state of the document can be recognized and the changes are traceable.

Adding annotations (e.g. notes, highlights) does not influence the document stored in the archive system. The archived documents can always be reproduced in their original version by hiding the annotations.

To ensure document versioning for changes to index information or application data, the user must guarantee proper definition of the following configuration parameters:

- The "LIFESTATE" system attribute of the document schema is set to the value "1";
- The "Modification in spite of archiving" parameter is set to the value "FALSE" for all index attributes within the document schema.

Requirement: Protecting personalized data

The German Federal Data Protection Law (Bundesdatenschutzgesetz – BDSG) requires that processing and saving personalized data is only allowed within the context of the legal provisions or through the consent of the person involved. It aims to protect individuals from impediments to their personal rights when using their personalized data.

The personalized data must be deleted after the retention period's expiration date or access to that data must be locked in case the data cannot be deleted or can be deleted only at great expenditure due to the specific type of storage (Clauses 20, 35 BDSG).

Findings:

Within the scope of our audit we ascertained that the application meets this requirement.

The application enables "locking document access" when allocating the corresponding authorizations by deleting the index information. Although documents containing personalized data continue to exist on the respective archiving medium, they can no longer be displayed or analyzed by document retrieval. Reorganization of this data from the container files to enable searching and displaying this data again is prevented by the program designed for reorganization.

3.2.3 Indexing and querying (Retrieval)

Requirement: Traceable and organized storage

The application must allow sufficient indexing or allocation of sort criteria, so that the data can be stored in a traceable and organized manner. Once allocated, indices should not be changed or deleted, or only be changed or deleted in a traceable manner.

Findings:

Within in the scope of our audit we ascertained that the application meets the requirements for traceable and unchangeable indexing.

Various types of documents can be defined and given a separate index structure by using schemas. The number of usable index attributes that can be filled with index values might be limited only by the relational database system used. This enables sufficient indexing and allocation of sort criteria. Each document is additionally stored under an automatically allocated system-wide unique primary key, i.e. "DOCUMENTID".

Index field contents are saved to the archiving medium both in the index database and along with the document. In case of unauthorized changes to indices in the index database or damage to the index database the original index entries may be restored by reorganizing the affected data container.

On the other hand, client applications also provide the option to change document index data. Provided that the document schema and the index attribute are properly configured (see Section 3.2.2), a new revision of the document is created so the original index is kept in a traceable version.

However, since index unchangeability is required for proper storage of documents subject to retention on electronic media, changes to the index must be prevented via the authorization concept and the suitable configuration of document schemas and index attributes for such documents. The effectiveness of protection must be monitored via suitable logs.

The application provides both the option to prevent changes to indices via the authorization concept and the option of revision-proof logging of all index changes.

Requirement: Proper indexing

It is necessary to store documents under a logical index in order to quickly access archived documents at a later stage. The application should support indexing to minimize the probability of document storage under incorrect or faulty search terms.

Findings:

Within the scope of our audit we determined that the application provides the required options to support reasonable and correct indexing.

The application allows both manual and automatic indexing (e.g. linking an index database, OCR, COLD, EASY for mySAP Level 2) of documents. Index fields can be declared as mandatory fields, multiple fields or predefined selection lists to enforce input or selection of defined terms. Additionally, date and number formats, for example, are checked on entering or attempting to archive documents, depending on the client used.

Requirement: Retrieval criteria

The application must provide appropriate tools to completely and quickly retrieve archived documents according to pre determined criteria.

Findings:

Our audit has shown that EASY ENTERPRISE.x and the checked additional components meet these requirements.

Stored documents can be retrieved by using the client applications EASYiDOX, EASYiDOX WEB and SAP Retrieval or from within the additional components EASY xBASE, EASY NOTES and EASY DOCUMENTS. The available functions basically provide the option to retrieve archived documents instantly and to display them.

We would like to point out that principally, a date range search must be performed when retrieving documents via the “archived at” system attribute, with the exception of the additional component EASY xBASE. The date range used during the search must be selected as one day greater than the actually viewed date range.

3.2.4 Reproduction

Requirement: Readable data

The application must provide the appropriate means to make archived documents readable in a timely and satisfactory manner.

Findings:

Our audit established that EASY ENTERPRISE.x meets the above requirements for reproducing documents.

Reproduction is either performed via the viewer integrated in the respective client or via the applications linked with the respective document type (e.g. Microsoft Power Point). We determine that in such a case no “save” operation can be performed, i.e. archived documents cannot be changed.

Requirement: Access restriction

Reproducing archived documents should be limited to authorized users.

Findings:

Our audit established that the application meets the requirements regarding user authorizations for reproducing documents.

The authorization concept enables limiting display permission for archived documents at various levels. The authorization for displaying documents can be limited to groups of document types (pools), individual document types (schemas) and at the level of individual index information (attributes).

3.3 Validating software security

3.3.1 Access protection

Requirement:

An effective access protection concept should ensure the segregation of duty during the process of document archiving, and prevent unauthorized access to data assets. This requires that suitable mechanisms are used for authenticating the user against the system components. At the same time, sufficient protection measures for the passwords used for authentication must be ensured.

Findings:

Within the scope of our audit we ascertained that EASY ENTERPRISE.x meets the requirements for access protection.

The user and authorization administration can be achieved both via EASY ENTERPRISE.x and via linking a third-party user management system such as Microsoft Active Directory using the LDAP standard protocol. The concept is based on the definition of permission roles and their assignment to users and document types. Authentication is necessary both when using the available client applications and for communication between individual components with the EASY ENTERPRISE.x server.

The administrative EE.x server functions and the additional components (EASY xBASE, EASY NOTES, EASY DOCUMENTS, EASY for mySAP) are also part of the user and authentication concept, and can thereby be protected from unauthorized access.

In addition, the application provides selected functions via command line programs (e.g. the “SpoolerImport” program). The system is accessed via calling methods and attributes at operating system level, i.e. access to a retrieval client is not required.

Within the scope of this audit we determined that access to the retrieval client, communication between additional components and the EE.x server, as well as starting security critical functions via the operating system’s command line (e.g. “SpoolerImport”) are properly protected through a password query. The user passwords are stored in an encrypted version in the configuration database when using the EE.x server functions.

A default user account including extensive authorizations that is required for installing the EASY ENTERPRISE.x Archive server exists. The initial password of that user is identical for all installations and therefore publicly known. The application’s documentation recommends changing the password; however, this is not enforced during installation. If the initial password is not changed, there will be a risk regarding unauthorized system access.

3.3.2 Data backup and recovery procedures

Requirement:

According to GoBS, proper handling of documents subject to retention, require adequate data backup procedures. The system should support various data backup procedures. Furthermore, it must be clearly documented which data assets require backup and on how to perform complete recovery of data assets.

Findings:

Our audit determined that EASY ENTERPRISE.x meets the requirements for data backup.

The data assets to be backed up are clearly structured and included in a traceable manner in the EASY ENTERPRISE.x server documentation. The provided information is sufficient to enable complete recovery.

EASY recommends backing up the index database. In case recovering a data backup should not be possible, the application provides functions enabling database recovery from the data containers stored on the archive media. A function test performed during this audit gave no cause for complaint.

3.3.3 Program development, maintenance and release

Requirement:

The procedure used for program development and the tools used should be documented in a traceable manner in written form. To avoid jeopardizing the quality of the existing program code through functional enhancements and error corrections, such a procedure should include at least the following steps:

- Written request for function enhancements or error corrections including release submitted by project management.
- Implementing the function enhancement or program correction by the development department.
- Testing and releasing the implemented function enhancement or the corrected functionality by the Quality Assurance department.
- Integration tests and release; as well as
- Complete release of the new or corrected version by project management.

Findings:

The Change Management procedure used by EASY is suitable for ensuring proper program development and maintenance.

The process implemented by EASY is divided into two partial areas:

- “Release management” as well as
- “Bug fixing and urgent feature requests”.

Both areas are sufficiently documented and are traceable in the form of process description by EASY. The “release management” process includes requirement management, release planning (incl. estimated enhancements, prioritizing, and resource planning), implementation, test and release procedure (individual tests and integration tests) as well as documentation and release activities. The “bug fixing and urgent feature requests” process is a simplified Change Management process consisting of the analysis, implementation, test and release activities. The simplified process is necessary to ensure fast response to critical errors. The test cases used in conjunction with Change Management are essentially based on automatic test scripts (about 11,000 individual tests) that enable fast, systematic and reproducible testing of application functions.

Using random samples, we determined that changes are traceable and are performed in compliance with the documented process.

The presented procedure controls the handling of program changes to all software products included in the audit scope, with the exception of the EASY DOCUMENTS and EASY WORKFLOW products, which were implemented by otris software AG, Dortmund, Germany, in compliance with EASY SOFTWARE specifications. This audit does not include the audit of the Change Management procedure used by otris software AG, Dortmund.

3.3.4 System communication and logging (Audit Trail)

Requirement: Protection of data transfer

In distributed systems huge data volumes are transferred via the network. Insofar as this communication is performed via public networks, the data needs to be protected against unauthorized access. The connections between the components should be encrypted for this.

Findings:

During our audit we carried out that data transfer between individual components is encrypted when properly configured and that the data is sufficiently protected against unauthorized access.

The Remote Method Invocation (RMI) and Hypertext Transfer Protocol (HTTP) protocols are used for component communication. Access via HTTP is implemented via a standard Web server, and can therefore be secured by using the HTTPS protocol at transport level. Communication via RMI (e.g. EASYiDOX) can also be secured by using SSL 3.0 when properly configuring the J2EE application server used.

Requirement: Logging processing errors / system activities

To enhance traceability of system-side processes, processing errors and system activities (e.g. creating, editing or deleting documents, faulty login attempts) should be automatically logged by the archive system.

Findings:

Within the scope of our audit we determined that EASY ENTERPRISE.x and the additionally checked components provide appropriate functions for logging processing errors and system activities.

EASY ENTERPRISE.x logs all system activities and errors in a central file on the archive server. The generated archive files can be displayed and filtered for analysis purposes by using the EASY Configuration Manager. In addition, regular backup of the generated log files in the archive system is ensured by the system.

The client applications considered for this audit and the additional components also include a log function. Within the scope of this audit, we were able to confirm the efficiency of this log function by viewing the application. Archiving the log files generated by the client application or the additional components must be ensured by organizational measures taken by the responsible users.

We would also point out that regular analysis of generated logs must be integrated into a functional organizational control environment of the responsible user.

3.4 Procedural documentation

Requirement:

In compliance with GoB/GoBS, documentation of an application must illustrate content, structure and the course of the procedure used completely and in a traceable manner. Procedural documentation on the part of the software provider must additionally include the description of the steps to be performed by the user for proper use of the processing functions and the changes to system settings by the user allowed by the application.

Findings:

Within the scope of our audit we determined that the documentation of the EASY ENTERPRISE.x application and the additionally audited components are appropriate and traceable.

For the purpose of our audit documented in this report, we essentially consulted the following documentation which comes with the EASY ENTERPRISE.x package and the respective additional components:

- Administrator's user guide (EEx-Configmanager_en.pdf),
- EASYiDOX user guide (EEx-RichClient_en.pdf),
- Web Client online help (EEx-WebClient_en.pdf),
- EASY CAPTURE user and administration guide (Cap_usr.pdf, Cap_adm.pdf),
- EASY xBASE user and configuration guide (EASY xBASE_en.pdf),
- EASY NOTES user guide (eenotesplus docu_en.pdf),
- EASY LOGISTICS CENTER Portal Manager (ELC-Reference User Guide.pdf),
- EASY LOGISTICS CENTER DOCUMENTS WORKFLOW (Workflow_Manual.pdf),
- EASY for mySAP Level 1, Level 2, SmartLink, and Retrieval (SapDoc_en.pdf, EEx_Level2_en.pdf, EEx_Smartlink_en.pdf, EEx_Retrieval_en.pdf).

Using sample program functions both from the processing functions and the system administration areas, a random check was made if the associated documentation is traceable, complete and factually correct.

Glossary

AO	Abgabenordnung (German Fiscal Code)
Client	Workstation or PC in a client-server environment
DMS	Document management system
FAIT 1	IDW Accounting Principle: Principles of Proper Accounting for the Use of Information Technology (IDW RS FAIT 1)
GDPdU	Basic Regulations for Accessing Data and Auditing Digital Documents (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen)
GoB	Generally Accepted Accounting Principles (Grundsätze ordnungsgemäßer Buchführung)
GoBS	Generally Accepted Accounting Principles in Computer-Assisted Accounting Systems, GAPCAS (Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme)
HGB	Handelsgesetzbuch (German Commercial Code)
IDW	Institut der Wirtschaftsprüfer (Institute of Certified Public Accountants)
Image	Visual representation of scanned original document
Index database	Integrated reference database; contains index information of documents stored or archived in the relational database
J2EE	Java 2 Enterprise Edition
Jukebox	Disk changer automaton for optical disks
LDAP	Lightweight Directory Access Protocol
OCR	Optical Character Recognition
JDBC	Java Database Connectivity. Sun specification of SQL-based query language for relational databases.
TIFF	Tagged Image File Format
WORM	Write Once Read Multiple

General Engagement Terms for Wirtschaftsprüfer and Wirtschaftsprüfungsgesellschaften [German Public Auditors and Public Audit Firms] as of January 1, 2002

This is an English translation of the German text, which is the sole authoritative version

1. Scope

(1) These engagement terms are applicable to contracts between Wirtschaftsprüfer [German Public Auditors] or Wirtschaftsprüfungsgesellschaften [German Public Audit Firms] (hereinafter collectively referred to as the "Wirtschaftsprüfer") and their clients for audits, consulting and other engagements to the extent that something else has not been expressly agreed to in writing or is not compulsory due to legal requirements.

(2) If, in an individual case, as an exception contractual relations have also been established between the Wirtschaftsprüfer and persons other than the client, the provisions of No. 9 below also apply to such third parties.

2. Scope and performance of the engagement

(1) Subject of the Wirtschaftsprüfer's engagement is the performance of agreed services — not a particular economic result. The engagement is performed in accordance with the Grundsätze ordnungsmäßiger Berufsausübung [Standards of Proper Professional Conduct]. The Wirtschaftsprüfer is entitled to use qualified persons to conduct the engagement.

(2) The application of foreign law requires — except for financial attestation engagements — an express written agreement.

(3) The engagement does not extend — to the extent it is not directed thereto — to an examination of the issue of whether the requirements of tax law or special regulations, such as, for example, laws on price controls, laws limiting competition and Bewirtschaftungsrecht [laws controlling certain aspects of specific business operations] were observed; the same applies to the determination as to whether subsidies, allowances or other benefits may be claimed. The performance of an engagement encompasses auditing procedures aimed at the detection of the defalcation of books and records and other irregularities only if during the conduct of audits grounds therefore arise or if this has been expressly agreed to in writing.

(4) If the legal position changes subsequent to the issuance of the final professional statement, the Wirtschaftsprüfer is not obliged to inform the client of changes or any consequences resulting therefrom.

3. The client's duty to inform

(1) The client must ensure that the Wirtschaftsprüfer — even without his special request — is provided, on a timely basis, with all supporting documents and records required for and is informed of all events and circumstances which may be significant to the performance of the engagement. This also applies to those supporting documents and records, events and circumstances which first become known during the Wirtschaftsprüfer's work.

(2) Upon the Wirtschaftsprüfer's request, the client must confirm in a written statement drafted by the Wirtschaftsprüfer that the supporting documents and records and the information and explanations provided are complete.

4. Ensuring independence

The client guarantees to refrain from everything which may endanger the independence of the Wirtschaftsprüfer's staff. This particularly applies to offers of employment and offers to undertake engagements on one's own account.

5. Reporting and verbal information

If the Wirtschaftsprüfer is required to present the results of the work in writing, only that written presentation is authoritative. For audit engagements the long-form report should be submitted in writing to the extent that nothing else has been agreed to. Verbal statements and information provided by the Wirtschaftsprüfer's staff beyond the engagement agreed to are never binding.

6. Protection of the Wirtschaftsprüfer's intellectual property

The client guarantees that expert opinions, organizational charts, drafts, sketches, schedules and calculations — especially quantity and cost computations - prepared by the Wirtschaftsprüfer within the scope of the engagement will be used only for his own purposes.

7. Transmission of the Wirtschaftsprüfer's professional statement

(1) The transmission of a Wirtschaftsprüfer's professional statement (long-form reports, expert opinions and the like) to a third party requires the Wirtschaftsprüfer's written consent to the extent that the permission to transmit to a certain third party does not result from the engagement terms. The Wirtschaftsprüfer is liable (within the limits of No. 9) towards third parties only if the prerequisites of the first sentence are given.

(2) The use of the Wirtschaftsprüfer's professional statements for promotional purposes is not permitted; an infringement entitles the Wirtschaftsprüfer to immediately cancel all engagements not yet conducted for the client.

8. Correction of deficiencies

(1) Where there are deficiencies, the client is entitled to subsequent fulfillment [of the contract]. The client may demand a reduction in fees or the cancellation of the contract only for the failure to subsequently fulfill [the contract]; if the engagement was awarded by a person carrying on a commercial business as part of that commercial business, a government-owned legal person under public law or a special government-owned fund under public law, the client may demand the cancellation of the contract only if the services rendered are of no interest to him due to the failure to subsequently fulfill [the contract]. No. 9 applies to the extent that claims for damages exist beyond this.

(2) The client must assert his claim for the correction of deficiencies in writing without delay. Claims pursuant to the first paragraph not arising from an intentional tort cease to be enforceable one year after the commencement of the statutory time limit for enforcement.

(3) Obvious deficiencies, such as typing and arithmetical errors and formelle Mängel [deficiencies associated with technicalities] contained in a Wirtschaftsprüfer's professional statements (long-form reports, expert opinions and the like) may be corrected — and also be applicable versus third parties — by the Wirtschaftsprüfer at any time. Errors which may call into question the conclusions contained in the Wirtschaftsprüfer's professional statements entitle the Wirtschaftsprüfer to withdraw — also versus third parties — such statements. In the cases noted the Wirtschaftsprüfer should first hear the client, if possible.

9. Liability

(1) *The liability limitation of § ["Article"] 323 (2) ["paragraph 2"] HGB [„Handelsgesetzbuch“: German Commercial Code] applies to statutory audits required by law.*

(2) *Liability for negligence; An individual case of damages*
If neither No. 1 is applicable nor a regulation exists in an individual case, pursuant to § 54a (1) no. 2 WPO [„Wirtschaftsprüferordnung“: Law regulating the Profession of Wirtschaftsprüfer] the liability of the Wirtschaftsprüfer for claims of compensatory damages of any kind — except for damages resulting from injury to life, body or health — for an individual case of damages resulting from negligence is limited to € 4 million; this also applies if liability to a person other than the client should be established. An individual case of damages also exists in relation to a uniform damage arising from a number of breaches of duty. The individual case of damages encompasses all consequences from a breach of duty without taking into account whether the damages occurred in one year or in a number of successive years. In this case multiple acts or omissions of acts based on a similar source of error or on a source of error of an equivalent nature are deemed to be a uniform breach of duty if the matters in question are legally or economically connected to one another. In this event the claim against the Wirtschaftsprüfer is limited to € 5 million. The limitation to the fivefold of the minimum amount insured does not apply to compulsory audits required by law.

(3) *Preclusive deadlines*

A compensatory damages claim may only be lodged within a preclusive deadline of one year of the rightful claimant having become aware of the damage and of the event giving rise to the claim - at the very latest, however, within 5 years subsequent to the event giving rise to the claim. The claim expires if legal action is not taken within a six month deadline subsequent to the written refusal of acceptance of the indemnity and the client was informed of this consequence. The right to assert the bar of the preclusive deadline remains unaffected. Sentences 1 to 3 also apply to legally required audits with statutory liability limits.

[Translator's notes are in square brackets]

10. Supplementary provisions for audit engagements

- (1) A subsequent amendment or abridgement of the financial statements or management report audited by a Wirtschaftsprüfer and accompanied by an auditor's report requires the written consent of the Wirtschaftsprüfer even if these documents are not published. If the Wirtschaftsprüfer has not issued an auditor's report, a reference to the audit conducted by the Wirtschaftsprüfer in the management report or elsewhere specified for the general public is permitted only with the Wirtschaftsprüfer's written consent and using the wording authorized by him. (2) If the Wirtschaftsprüfer revokes the auditor's report, it may no longer be used. If the client has already made use of the auditor's report, he must announce its revocation upon the Wirtschaftsprüfer's request. (3) The client has a right to 5 copies of the long-form report. Additional copies will be charged for separately.

11. Supplementary provisions for assistance with tax matters

- (1) When advising on an individual tax issue as well as when furnishing continuous tax advice, the Wirtschaftsprüfer is entitled to assume that the facts provided by the client — especially numerical disclosures — are correct and complete; this also applies to bookkeeping engagements. Nevertheless, he is obliged to inform the client of any errors he has discovered. (2) The tax consulting engagement does not encompass procedures required to meet deadlines, unless the Wirtschaftsprüfer has explicitly accepted the engagement for this. In this event the client must provide the Wirtschaftsprüfer, on a timely basis, all supporting documents and records — especially tax assessments — material to meeting the deadlines, so that the Wirtschaftsprüfer has an appropriate time period available to work therewith. (3) In the absence of other written agreement, continuous tax advice encompasses the following work during the contract period:
- preparation of annual tax returns for income tax, corporation tax and business tax, as well as net worth tax returns on the basis of the annual financial statements and other schedules and evidence required for tax purposes to be submitted by the client
 - examination of tax assessments in relation to the taxes mentioned in (a)
 - negotiations with tax authorities in connection with the returns and assessments mentioned in (a) and (b)
 - participation in tax audits and evaluation of the results of tax audits with respect to the taxes mentioned in (a)
 - participation in Einspruchs- und Beschwerdeverfahren [appeals and complaint procedures] with respect to the taxes mentioned in (a).

In the afore-mentioned work the Wirtschaftsprüfer takes material published legal decisions and administrative interpretations into account.

- (4) If the Wirtschaftsprüfer receives a fixed fee for continuous tax advice, in the absence of other written agreements the work mentioned under paragraph 3 (d) and (e) will be charged separately. (5) Services with respect to special individual issues for income tax, corporate tax, business tax, valuation procedures for property and net worth taxation, and net worth tax as well as all issues in relation to sales tax, wages tax, other taxes and dues require a special engagement. This also applies to:
- the treatment of nonrecurring tax matters, e. g. in the field of estate tax, capital transactions tax, real estate acquisition tax
 - participation and representation in proceedings before tax and administrative courts and in criminal proceedings with respect to taxes, and
 - the granting of advice and work with respect to expert opinions in connection with conversions of legal form, mergers, capital increases and reductions, financial reorganizations, admission and retirement of partners or shareholders, sale of a business, liquidations and the like.

- (6) To the extent that the annual sales tax return is accepted as additional work,

this does not include the review of any special accounting prerequisites nor of the issue as to whether all potential legal sales tax reductions have been claimed. No guarantee is assumed for the completeness of the supporting documents and records to validate the deduction of the input tax credit.

12. Confidentiality towards third Parties and data security

- (1) Pursuant to the law the Wirtschaftsprüfer is obliged to treat all facts that he comes to know in connection with his work as confidential, irrespective of whether these concern the client himself or his business associations, unless the client releases him from this obligation. (2) The Wirtschaftsprüfer may only release long-form reports, expert opinions and other written statements on the results of his work to third parties with the consent of his client. (3) The Wirtschaftsprüfer is entitled - within the purposes stipulated by the client - to process personal data entrusted to him or allow them to be processed by third parties.

13. Default of acceptance and lack of cooperation on the part of the client

If the client defaults in accepting the services offered by the Wirtschaftsprüfer or if the client does not provide the assistance incumbent on him pursuant to No. 3 or otherwise, the Wirtschaftsprüfer is entitled to cancel the contract immediately. The Wirtschaftsprüfer's right to compensation for additional expenses as well as for damages caused by the default or the lack of assistance is not affected, even if the Wirtschaftsprüfer does not exercise his right to cancel.

14. Remuneration

- (1) In addition to his claims for fees or remuneration, the Wirtschaftsprüfer is entitled to reimbursement of his outlays: sales tax will be billed separately. He may claim appropriate advances for remuneration and reimbursement of outlays and make the rendering of his services dependent upon the complete satisfaction of his claims. Multiple clients awarding engagements are jointly and severally liable. (2) Any set off against the Wirtschaftsprüfer's claims for remuneration and reimbursement of outlays is permitted only for undisputed claims or claims determined to be legally valid.

15. Retention and return of supporting documentation and records

- (1) The Wirtschaftsprüfer retains, for seven years, the supporting documents and records in connection with the completion of the engagement — that had been provided to him and that he has prepared himself — as well as the correspondence with respect to the engagement. (2) After the settlement of his claims arising from the engagement, the Wirtschaftsprüfer, upon the request of the client, must return all supporting documents and records obtained from him or for him by reason of his work on the engagement. This does not, however, apply to correspondence exchanged between the Wirtschaftsprüfer and his client and to any documents of which the client already has the original or a copy. The Wirtschaftsprüfer may prepare and retain copies or photocopies of supporting documents and records which he returns to the client.

16. Applicable law

Only German law applies to the engagement, its conduct and any claims arising therefrom.