

The certification body of TÜV Informationstechnik GmbH  
hereby awards this certificate to the company

**SIZ Informatikzentrum der  
Sparkassenorganisation GmbH  
Simrockstraße 4  
53113 Bonn, Germany**

to confirm that its software

**Sicherer IT-Betrieb, Basisvariante,  
Version 8.0**

fulfils all requirements of the criteria

**Trusted Product ISO 27001 Tool,  
Version 1.0**

of TÜV Informationstechnik GmbH. The requirements are  
summarized in the appendix to this certificate. The appendix is  
part of the certificate and consists of 4 pages. The certificate is  
valid only in conjunction with the corresponding evaluation report  
until 2012-05-31.



© 2010 TÜVIT GmbH - Member of TÜV NORD Group

Certificate Registration No.:  
TUVIT-PQ6117.10

12

Essen, 2010-06-07

Dr. Christoph Sutter  
Head of Certification Body

**TÜV Informationstechnik GmbH**  
Member of TÜV NORD Group  
Langemarckstr. 20  
45141 Essen, Germany  
www.certuvit.de

**Certificate**

## **Certification System**

The certification body of TÜViT GmbH performs certification on the basis of the following product certification system:

- German document: “Zertifizierungsschema für TÜViT Trusted-Zertifikate der Zertifizierungsstelle TÜV Informationstechnik GmbH“, version 1.0 as of 2010-05-18, TÜViT GmbH

## **Evaluation Report**

- “Prüfbericht Trusted Product ISO/IEC 27001:2005 Tool – Sicherer IT-Betrieb, Basisvariante, Version 8.0”, Version 1.2 as of 2010-06-01, Report ID: PQ6117.10\_PB\_V1-2.doc, TÜViT GmbH

## **Evaluation Requirements**

- Trusted Product ISO 27001 Tool, Version 1.0

## **Evaluation Target**

- Sicherer IT-Betrieb, Basisvariante Version 8.0

## **Evaluation Result**

- The target of evaluation fulfils all applicable evaluation requirements.
- The certification requirements defined in the certification system are fulfilled.

## Summary of the Evaluation Requirements

### 1 Coverage to ISO/IEC 27001

A requirements catalogue specifies the functional requirements of the ISO 27001 tool and demonstrates that ISO/IEC 27001 is completely covered. The ISO 27001 tool completely covers and complies with the functionality specified within the requirements catalogue and the full ISO/IEC 27001 standard.

### 2 Tool support during all ISMS<sup>1</sup> phases

The ISO 27001 tool covers all phases specified by the ISO/IEC 27001 standard, i. e. the full Plan-Do-Check-Act (PDCA) cycle is covered.

### 3 Management of ISMS documents

An administrative system for the documentation of the ISMS and a system for the control of documents and records are provided.

### 4 Help system

The ISO 27001 tool offers a help system which supports the user regarding the operation of the tool and the application of the ISO/IEC 27001 standard. The help system of the ISO 27001 tool includes a user manual for the tool operation and lists of important aspects to be considered within related phases of the ISMS.

### 5 Search system

The search system of the ISO 27001 tool enables the user to search for documents within the tool as well as to carry out a buzzword search within documents.

---

<sup>1</sup> Information management security system according to ISO/IEC 27001

## **6 System for date and activity tracing**

The system for date and activity tracing of the ISO 27001 tool informs the user about progress and the status of activities.

## **7 Risk methodology**

The risk methodology supplied with the ISO 27001 tool completely and correctly covers the functionalities of the ISO/IEC 27001 standard. The supplied risk methodology can be replaced by an individual, company-owned methodology.

## **8 Controls described in Annex A of the ISO/IEC 27001**

The controls described in Annex A of the ISO/IEC 27001 standard form an integral part of the ISO 27001 tool. Self-defined controls can be added.

## **9 Planning of internal audit conduct**

The ISO 27001 tool supports the user in time and content planning of internal audits, i. e. the internal audit program plan fully covers the ISO/IEC 27001 standard.

## **10 Resource Management**

The ISO 27001 tool offers the option to enter and visualize resources which are required within different phases of the establishment of an ISMS.

## **11 Authentication system / user administration**

The ISO 27001 tool includes a role-based authentication system and a user administration (using a carrier platform, if required).

## **12 Support of different standards**

The ISO 27001 tool enables the integration of different standards (ISO/IEC 27001, ISO/IEC 27002) and different versions of a particular standard.

### **13 Current state of information security**

**TÜV**<sup>®</sup>

The ISO 27001 tool is state-of-the-art regarding selected aspects of information security.

### **14 Software development process**

The software of the ISO 27001 tool is state-of-the-art regarding the software development process and the related documentation. Principles, methods and tools for the development of software systems according to the division of tasks and engineering principles are used systematically. The software development process is quality-assured.