

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH  
bescheinigt hiermit dem Unternehmen

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

für die Software

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

die Erfüllung aller Anforderungen der Kriterien

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

der TÜV Informationstechnik GmbH. Die Prüfanforderungen sind in der Anlage zum Zertifikat zusammenfassend aufgelistet. Die Anlage zum Zertifikat ist Bestandteil des Zertifikats und besteht aus 4 Seiten. Dieses Zertifikat gilt nur in Verbindung mit dem zugehörigen Prüfbericht und ist bis zum 31.05.2012 gültig.



Zertifikat-Registrier-Nr.:  
TUVIT-PQ6117.10

12

© 2010 TÜVIT GmbH - Member of TÜV NORD Group

Essen, 07.06.2010

Dr. Christoph Sutter  
Leiter Zertifizierungsstelle

**TÜV Informationstechnik GmbH**  
Unternehmensgruppe TÜV NORD  
Langemarckstraße 20  
45141 Essen  
www.certuvit.de

Zertifikat

## Zertifizierungssystem

TÜV<sup>®</sup>

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH führt Zertifizierungen auf der Basis des folgenden Produkt-Zertifizierungssystems durch:

- “Zertifizierungsschema für TÜViT Trusted-Zertifikate der Zertifizierungsstelle TÜV Informationstechnik GmbH“, Version 1.0 vom 18.05.2010, TÜViT GmbH

## Prüfbericht

- „*Prüfbericht Trusted Product ISO/IEC 27001:2005 Tool – Sicherer IT-Betrieb, Basisvariante, Version 8.0*“, Version 1.2 vom 01.06.2010, Report ID: PQ6117.10\_PB\_V1-2.doc, TÜViT GmbH

## Prüfanforderungen

- Trusted Product ISO 27001 Tool, Version 1.0

## Prüfgegenstand

- Sicherer IT-Betrieb, Basisvariante, Version 8.0

## Prüfergebnis

- Der Prüfgegenstand erfüllt alle anwendbaren Anforderungen aus den Prüfkriterien.
- Die im Zertifizierungssystem definierten Zertifizierungsvoraussetzungen sind erfüllt.

## **Zusammenfassung der Prüfanforderungen**

**TÜV**<sup>®</sup>

### **1 Abdeckung der ISO/IEC 27001**

Es existiert ein funktionaler Anforderungskatalog zum ISO 27001 Tool, aus dem ersichtlich ist, dass die ISO/IEC 27001 vollständig abgedeckt ist. Die im Katalog spezifizierte Funktionalität und die gesamte Norm ISO/IEC 27001 werden durch das Tool vollständig und richtig abgedeckt.

### **2 Tool-Unterstützung in allen Phasen des ISMS<sup>1</sup>**

Das ISO 27001 Tool deckt alle, von der ISO/IEC 27001 spezifizierten Phasen, d. h. den gesamten Plan-Do-Check-Act (PDCA)-Zyklus, ab.

### **3 Verwaltung von ISMS-Dokumenten**

Es existiert ein Verwaltungssystem für die Dokumentation des ISMS und ein System zur Lenkung von Dokumenten und Aufzeichnungen.

### **4 Hilfesystem**

Es existiert ein Hilfesystem im ISO 27001 Tool, das den Anwender bei der Bedienung des Tools und bei der Anwendung der ISO/IEC 27001 unterstützt. Das Hilfesystem des Tools enthält ein Benutzerhandbuch zur Tool-Bedienung und Auflistungen mit wichtigen Aspekten, die in der jeweiligen Phase des ISMS insbesondere zu berücksichtigen sind.

### **5 Suchsystem**

Es existiert ein Suchsystem im ISO 27001 Tool, das dem Anwender sowohl die Suche von Dokumenten innerhalb des Tools als auch die Stichwortsuche innerhalb von Dokumenten ermöglicht.

---

<sup>1</sup> Informationssicherheits-Managementsysteme nach ISO/IEC 27001

## **6 Termin- und Aktivitätsverfolgung**

Es existiert ein System zur Termin- und Aktivitätsverfolgung im ISO 27001 Tool, das den Anwender hinsichtlich Fortschritt und Status von Aktivitäten informiert.

## **7 Risikomethodik**

Die mit dem ISO 27001 Tool mitgelieferte Risikomethodik deckt die diesbezüglichen Anforderungen der ISO/IEC 27001 vollständig und funktional richtig ab. Der Austausch der mitgelieferten Risikomethodik durch eine individuelle, unternehmenseigene Methodik ist möglich.

## **8 Maßnahmen des Anhang A der ISO/IEC 27001**

Die Maßnahmen des Anhangs A der ISO/IEC 27001 sind Bestandteil des ISO 27001 Tools. Es besteht die Möglichkeit, selbst definierte Maßnahmen im Tool zu ergänzen.

## **9 Planung interner Audits**

Das ISO 27001 Tool unterstützt den Anwender bei der zeitlichen Planung und inhaltlichen Konzeptionierung interner Audits, so dass das konzipierte interne Auditprogramm die ISO/IEC 27001 vollständig abdeckt.

## **10 Ressourcenverwaltung**

Ressourcen, die in den verschiedenen Phasen der Etablierung eines ISMS benötigt werden, können im ISO 27001 Tool eingegeben und angezeigt werden.

## **11 Berechtigungssystem / Benutzerverwaltung**

Das ISO 27001 Tool verfügt (ggf. unter Verwendung einer Trägerplattform) über ein Rollen-basiertes Berechtigungssystem und eine Benutzerverwaltung.

## **12 Unterstützung von verschiedenen Normen**

**TÜV**<sup>®</sup>

Das ISO 27001 Tool ermöglicht die Integration verschiedener Normen (ISO/IEC 27001, ISO/IEC 27002) und verschiedener Versionen einer Norm.

## **13 Aktueller Stand der Informationssicherheit**

Das ISO 27001 Tool ist hinsichtlich ausgewählter Aspekte der Informationssicherheit auf dem aktuellen Stand der Technik.

## **14 Software-Entwicklungsprozess**

Die Software des ISO 27001 Tools ist hinsichtlich des Software-Entwicklungsprozesses und der zugrundeliegenden Dokumentation auf dem aktuellen Stand der Technik. Es erfolgt eine systematische Verwendung von Prinzipien, Methoden und Werkzeugen für die arbeitsteilige, ingenieurmäßige Entwicklung von Softwaresystemen. Der Software-Entwicklungsprozess ist qualitätsgesichert.