T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting 2011

Sicherer IT-Betrieb
Ein Ansatz zum ganzheitlichen Informationssicherheits-Management

Dr. Detlef Reich
SIZ GmbH
Senior-Berater Informationssicherheit

INFORMATIKZENTRUM
DER SPARKASSEN-
ORGANISATION GMBH

Sicherer IT-Betrieb

Produkt für ein ganzheitliches Informationssicherheits-Management

Name
Dr. Detlef Reich

TISP-Community-Meeting, Berlin 07.11.2011

SIZ Vorstellung

Motivation zur Informationssicherheit

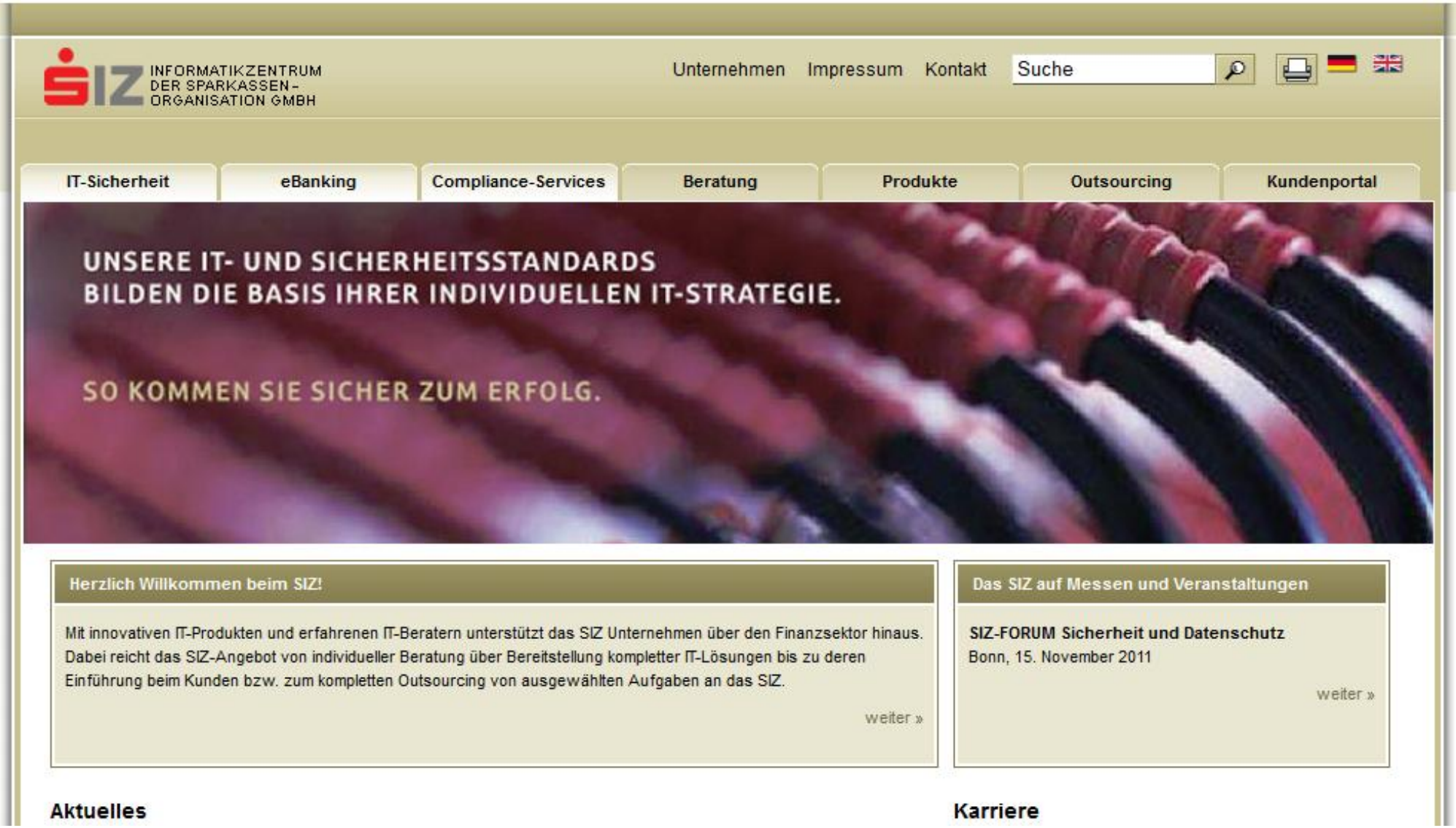
Produkt Sicherer IT-Betrieb

Prozess ISMS

Dokumentationswerkzeug

Zusammenfassung

Unsere Mitarbeiter setzen seit 1990 Maßstäbe in IT-Sicherheits- und eBanking-Standards in der Finanzwirtschaft und darüber hinaus und bieten passende IT-Beratung und -Produkte.



Neben der Sparkassen-Finanzgruppe gehören andere Kreditinstitute, Versicherer, Banken, IT und TK-Dienstleister sowie Industrieunternehmen zu unseren Kunden

SÜDWESTBANK
Leistung ist im Süden zu Hause.

GAD
IT für Banken

mdr

HypoVereinsbank

KÄSSBOHRER GELÄNDEFAHRZEUG AG

Uhlmann

Weltmarktführer für Verpackungsmaschinen der Pharmaindustrie

Bundesamt für Sicherheit in der Informationstechnik

enisa
European Network and Information Security Agency

schufa

DATEV

.comdirect

VISA

T · · Mobile

swissgrid

T · · Systems

symantec.
Deutschland, Schweiz und Österreich

opta data

COMMERZBANK

ZENTRALER KREDITAUSSCHUSS

Gemeinsam mit unseren Kunden entwickeln wir eine individuelle IT-Steuerung – bezogen auf deren vorhandene IT-Infrastruktur und abgestimmt für einen reibungslosen und wirtschaftlichen Betrieb

IT-Management

IT-Steuerungskompetenz für reibungslose Abläufe

Gemeinsam mit Ihnen entwickeln wir eine individuelle IT-Steuerung, die auf Ihre vorhandene IT-Infrastruktur abgestimmt ist und Ihnen einen reibungslosen und wirtschaftlichen Betrieb ermöglicht.

» » IT-Steuerung - Instrumente «

Control IT stellt die methodische Basis der IT-Steuerung dar. Wir unterstützen Sie dabei, Ihre IT-Steuerung durch eine individuelle Umsetzung dieser Methodik zum Erfolg zu führen.

weiter lesen ►

» » Business Continuity «

"Noah hat die Arche nicht erst erbaut, als es anfing zu regnen!" Wir bieten Ihnen mit einer bewährten Methodik und einem integrierbaren Produkt eine Lösung zur proaktiven Absicherung Ihrer Kerngeschäftsprozesse.

weiter lesen ► | Produkte ►

» » Notfallplanung «

Die Aufrechterhaltung wesentlicher Geschäftsfunktionen ist ein wichtiger Erfolgsfaktor in Ausnahmesituationen und Notfällen. Die Vermeidung kritischer Unterbrechungen und Folgen setzt das Beherrschen der Notfallverfahren und deren Wirksamkeit voraus.

weiter lesen ►

» » IT-Revision «

Die Anforderungen an die IT-Revision steigen durch die Vielfalt der zu untersuchenden Themen und deren Komplexität kontinuierlich an. Mit einem modular aufgebauten Leistungsangebot unterstützen wir Ihre IT-Revision.

weiter lesen ► | Produkte ►

Wir bieten Ihrer IT den besten Schutz – mit unseren zukunfts-fähigen, praxisgerechten und prozessorientierten Lösungen für die Informationssicherheit in der Finanzwirtschaft und darüber hinaus

IT-Sicherheit

Bieten Sie Ihrer IT den besten Schutz.

Wir setzen Maßstäbe für zukunftsfähige, praxisgerechte und prozessorientierte Informationssicherheit in der Finanzwirtschaft, bei Versicherungen und in Unternehmen.

Beratung IT-Sicherheit

Erfahrung ist der Schlüssel zu optimalen Ergebnissen. Wir bieten nicht nur Produkte, sondern unsere hochqualifizierten Mitarbeiter helfen Ihnen auch direkt bei der Umsetzung Ihrer individuellen Herausforderungen.

weiter lesen ► | Produkte ►

Sicherheitsanalysen

Wir unterstützen Sie bei der Analyse Ihrer Sicherheitsrisiken. Hierzu führen wir bei Ihnen praxisgerechte und wirtschaftlich effiziente Sicherheits-Audits durch.

weiter lesen ► | Produkte ►

Notfallübungen

Erst die Übung macht den Meister! Geschäftsfortführungs- und IT-Notfallpläne müssen erprobt sein, um sicherzustellen, dass im Ernstfall alles funktioniert.

weiter lesen ► | Produkte ►

Informationssicherheit

Unser Produkt "Sicherer IT-Betrieb" bildet bei rund 400 Kunden die Basis für deren Informationssicherheits-Managementsystem (ISMS).

weiter lesen ► | Produkte ►

Zertifizierung

Im Rahmen eines Zertifizierungsprozesses bescheinigen wir den erfolgreichen Betrieb eines Informationssicherheits-Managementssystems auf Basis unseres Produkts "Sicherer IT-Betrieb".

weiter lesen ► | Produkte ►

Computer-Notfallteam

Bei Angriffen auf Ihre IT-Systeme ist eine schnelle und fachkundige Reaktion entscheidend. Fast noch wichtiger ist präventives und nachhaltiges Handeln. Unser CERT unterstützt Sie dabei.

weiter lesen ► | Produkte ►

Unsere erprobten und effizienten Lösungen führen Sie schnell zu einer best-practice ISMS-Baseline, die bedarfsgerecht und einfach ausgebaut werden kann

- Gesetzes-Konformität
- Konformität zu relevanten Standards
- angemessene und erprobte Grundlage für eine Zertifizierung
- praktikabel und praxiserprobt

Zertifizierung

Optimierung der Sicherheit (optionale Maßnahmen)

- IT-Notfall (Planung/Test)
- IT-System-Audits
- Penetrations-tests
- Support für Interne Revision
- BCM / BCP (Planung/Test)
- CERT
- (ggf. weitere)

ISMS-Baseline: Sicherer IT-Betrieb

- Definition ISMS-Scope
- Inventar der IT-Werte
- Basis-Reports für IT-Risiken
- Maßnahmen-plan
- ISMS-Prozess und Organisation
- Basis-Analyse der IT-Risiken
- Soll-Ist-Vergleich & Risiken
- (ggf. weitere)

SIZ Vorstellung

Motivation zur Informationssicherheit

Produkt Sicherer IT-Betrieb

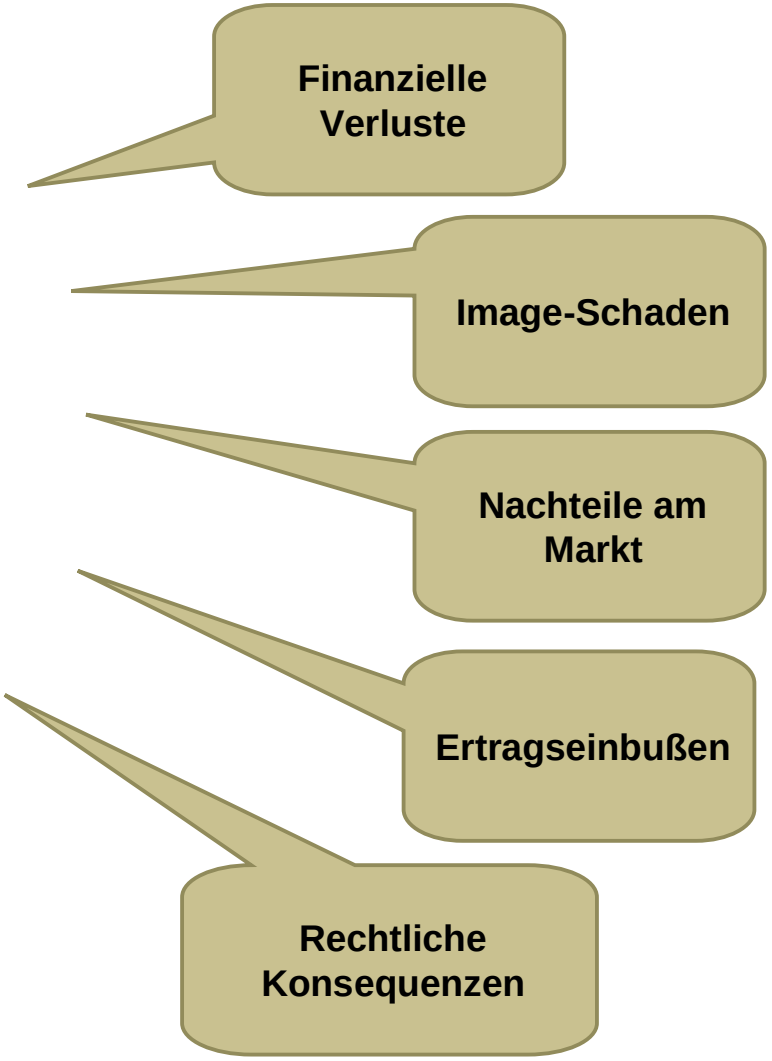
Prozess ISMS

Dokumentationswerkzeug

Zusammenfassung

Verfügbarkeit, Integrität und Vertraulichkeit von Informationen sind für Unternehmen erfolgsentscheidende Faktoren

- Anforderungen an Geschäftsprozesse
  - Zeitnahe Abwicklung
  - Aktuelle und korrekte Informationen
  - Vertraulicher Umgang mit Informationen
  - Wirtschaftlichkeit
  - Gesetzeskonformität und Prüfungsanforderungen (IT-Compliance)
  - Flexibilität
- Störungen in den Prozessabläufen können zu schwerwiegende Konsequenzen führen



Neben den Anforderungen zur reinen Abwicklung der Geschäftsprozesse gibt es noch Weitere

- Deutsche Gesetze, Anforderungen von Aufsichtsbehörden
  - Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
  - Handelsgesetzbuch (HGB) sowie GoB, GoBS
  - Grundsätze zum Datenzugriff und zur Prüfbarkeit dig. Unterlagen (GDPdU)
  - Bundesdatenschutzgesetz (BDSG)
  - Telemediengesetz (TMG)
  - Telekommunikationsgesetz (TKG)
  - Strafgesetzbuch (StGB)
- Stellungnahmen, Prüfungsstandards- und -hinweise der Wirtschaftsprüfer
- ISO / IEC 27001, 27002, 27003, 27004, 27005
- COBIT
- Verträge

Informationen und IT-Infrastruktur sind die Basis heutiger Geschäftsmodelle

- Unternehmen sind in nahezu allen Bereichen massiv von einer reibungslos und sicher funktionierenden IT-Infrastruktur abhängig
- Anforderungen seitens des Gesetzgebers und der Aufsichtsorgane erhöhen sich, die zunehmend bis auf die informationstechnologischen Komponenten der Unternehmen durchschlagen
- Die IT ist immer vielfältigeren Bedrohungen und zahlreicheren Angriffen ausgesetzt
- Einhaltung von Standards als Qualitätsmerkmal

- Daher wird eine Lösung benötigt, bei der Sicherheit, Betrieb und Wirtschaftlichkeit im Einklang stehen

SIZ Vorstellung

Motivation zur Informationssicherheit

Produkt Sicherer IT-Betrieb

Prozess ISMS

Dokumentationswerkzeug

Zusammenfassung

Der Standard „Sicherer IT-Betrieb“ ist eine Plattform für ein ganzheitliches Informationssicherheits-Management

- Ganzheitlicher Ansatz zum Informationssicherheits- und IT-Risikomanagement
- Lebenszyklus der Informationssicherheit und des IT-Betriebs wird vollständig abgedeckt
- Risikoorientierter Ansatz für wirtschaftlich sinnvolle und angemessene Lösungen
- Alle Ebenen im Unternehmen, von der Geschäftsführung bis zum Nutzer und Techniker, werden adressiert
- Harmoniert mit gängige Standards wie
  - ISO/IEC 27001:2005,
  - BSI Schichtenmodell,
  - CobiT,
  - IDW,
  - ITIL und
  - weiteren (branchenspezifischen) Standards

Basisvariante, V8.0 zertifiziert als

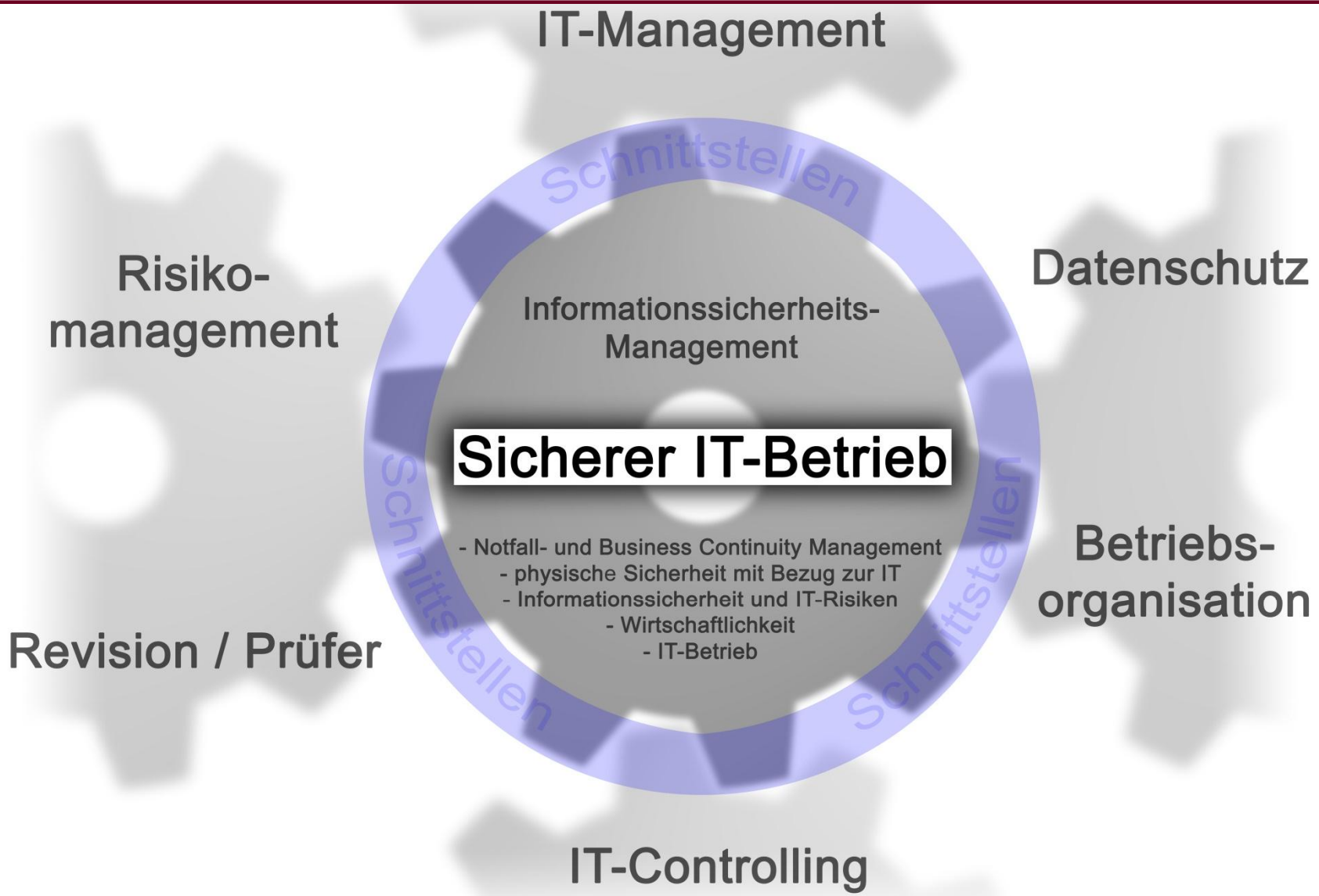
ISO 27001 Tool PQ6117.10 TÜViT® 2010 Trusted Product Voluntary Validation

Der Standard „Sicherer IT-Betrieb“ erprobtes System für das Informationssicherheits-Management

- Kontinuierliche Weiterentwicklung des Produkts und Aktualisierung der Inhalte seit über 10 Jahren

- Informationssicherheits-Management auf Basis „Sicherer IT-Betrieb“ wurde inzwischen bei über 400 Unternehmen im In- und Ausland etabliert. Hierzu gehören:
  - Sparkassen, Banken und Landesbanken
  - (öffentlichen) Versicherungen
  - Rechenzentren, (Finanz-)Dienstleistern
  - weitere Unternehmen

"Sicherer IT-Betrieb" - ganzheitlicher Ansatz zum Informationssicherheits- und IT-Risikomanagement



Das Produkt "Sicherer IT-Betrieb" deckt den gesamten Lebenszyklus der Informationssicherheit und des IT-Betriebs ab

- **Prozessunterstützung**
  für den Informationssicherheits-Beauftragten
  inkl. Hilfsmitteln, wie Leitfäden, Formularen oder Mustern

- **Nachschlagewerk**
  für das Informationssicherheits- und IT-Risikomanagement

  Vollständige und aktuelle Aufstellung aller für Informationssicherheit und IT-Betrieb zu beachtenden Kriterien und Regelungsbedarfe (Gesetze, Normen, Compliance-Themen)

- **Dokumentationsplattform**
  werkzeugunterstütze Einbindung und Auswertung von eigenen Dokumenten und Auditergebnissen bzw. Risikobehandlung

Informationssicherheits-Risiken treten nicht nur in der IT auf - ein ganzheitlicher Ansatz zu deren Reduzierung und Steuerung ist daher notwendig

Mittels Kategorien, Unterkategorien und Konzepten sind die Inhalte strukturiert. Dabei werden auch die Schnittstellen zum ISMS betrachtet.

- Organisatorische Konzepte

  IS-Organisation, IS-Risikomanagement, Dokumentation, Inventarisierung, Archivierung, Schulung / Sensibilisierung, Audit

- Logische, technische Konzepte

  Nutzerverwaltung, Schadsoftware / schadhafte Inhalte, Netzstruktur und -sicherheit, Protokollierung, Härtung, Datenaustausch und –ablage, Virtualisierung

- Physische Konzepte

  Standort- und Raumfaktoren, Strom / Blitz / Klima, Brandschutz, Zutrittsschutz und Überwachung

- Konzepte Notfallbehandlung

  Geschäftsfortführung, Notfallorganisation, Notfallplan

- Betriebskonzepte

  Kapazitäts- und Verfügbarkeitsmanagement, Datensicherungsmanagement, Change- und Releasemanagement, Incident- und Problemmanagement

- Konzepte Vertragsbeziehung

  Vertragsgestaltung, Details der Regelungen, Überwachung der Regelungen

- Konzepte ISMS-Schnittstellen

  Schnittstelle IT-Management, Schnittstelle Kontrollsysteme, Schnittstelle Risikomanagement, Schnittstelle Datenschutz, Schnittstelle Personal

Systematisch aufgebaute Konzepte definieren die Anforderungen an einen sicheren IT-Betrieb

- Konzepte beinhalten die Anforderungen aus Gesetze, Normen, (IT-)Compliance-Themen, sowie „best practice“-Ansätzen
- Gesetzliche und andere regulatorischen Anforderungen werden klar von Handlungsempfehlungen unterschieden
- Bedrohungspotentiale werden anhand eines Bedrohungskatalogs aufgezeigt, dessen Inhalte sich an gängige Standards (z. B. ISO 27005:2008, CobiT, BSI-Standard 100-3) anlehnen
- Zusätzlich werden konzeptabhängig Umsetzungshilfen angeboten

K001 Verantwortlichkeiten

Oberthema: Konzepte > Organisatorische Konzepte > IS-Organisation

| Umsetzung | Ziel | Beschreibung | Auditergebnis | Bedrohungspotential | Themen und Rollen | Umsetzungshilfen |

Ziel

Klare Definition der Verantwortlichen und ihrer Rollen im Informationssicherheits-Management (ISMS)

Beschreibung

Unternehmensführung

Die Unternehmensführung sollte im Bereich Informationssicherheit sichtbares Engagement zeigen, indem sie entsprechende Sensibilisierungs-Programme initiiert und unterstützt oder indem sie sich selbst bei Bedarf, Anfragen, Problemen etc. an das Informationssicherheits-Management wendet. Sie

Datenschutz überprüft und abgestimmt werden.

- Weitere typische Rollen, die regelmäßig oder bei Bedarf im Informationssicherheits-Management beteiligt sind: Revisor, Brandschutzbeauftragter, Haustechnik, Manager operationelle Risiken, Notfallbeauftragter.

Bedrohungspotential

- B001 Verstoß gegen Gesetze / Vorschriften
- B004 unzureichende Handlungsfähigkeit bei Notfällen
- B011 Nichterkennen von Risiken

Siehe auch: Bedrohungen

Umsetzungshilfen

Umsetzungshilfen zu K001 Verantwortlichkeiten

SIZ Vorstellung

Motivation zur Informationssicherheit

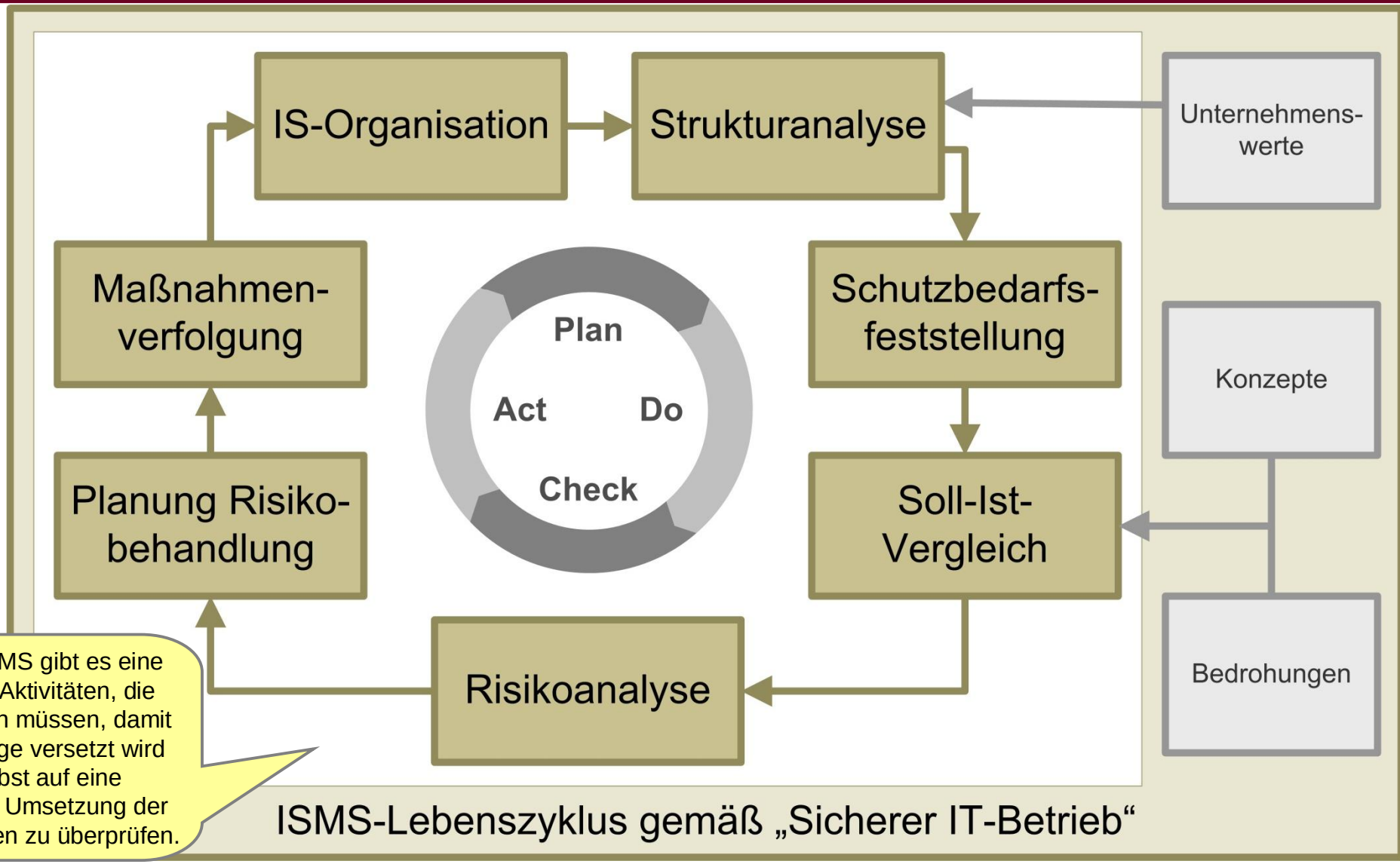
Produkt Sicherer IT-Betrieb

Prozess ISMS

Dokumentationswerkzeug

Zusammenfassung

„Sicherer IT-Betrieb“ zeigt nicht nur „Was“ umgesetzt werden muss, sondern auch „Wie“ der Prozess optimal realisiert werden kann



ISMS-Lebenszyklus gemäß „Sicherer IT-Betrieb“

In einem ISMS gibt es eine Reihe von Aktivitäten, die realisiert sein müssen, damit es in die Lage versetzt wird sich selbst auf eine vollständige Umsetzung der Anforderungen zu überprüfen.

Der Standard „Sicherer IT-Betrieb“ ist prozessorientiert und beschreibt die Aktivitäten zur Etablierung und den Betrieb des ISMS

- Aktivitäten geben über die Konzepte hinaus Hilfestellungen für die typischen Abläufe in der Praxis
- Aktivitäten beschreiben typische, alltägliche bzw. wiederkehrende Abläufe, die verschiedene Anforderungen des Informationssicherheits-Managements erfüllen müssen
- Aktivitäten umfassen sowohl eine Handlungsanweisung zu einer Tätigkeit, wie auch die dazu benötigten Hilfsmittel

A001 IS-Organisation pflegen

Oberthema: Prozess Informationssicherheits-Management > Aktivitäten > Aktivitäten zu Unternehmensprozessen

Umsetzung

Beschreibung

- Definition der Informationssicherheits-Organisation in Form einer Informationssicherheits-Leitlinie, mit der die Informationssicherheit im Unternehmen verankert werden sollen. Dabei
- Inkraftsetzung der Informationssicherheits-Leitlinie durch die Unternehmensführung

Turnus

Die Überprüfung sollte regelmäßig, aber mindestens einmal jährlich erfolgen.

Vorgehensweise

Für die konkrete Umsetzung sind folgende Hilfsmittel hinterlegt:

- **Informationssicherheits-Leitlinie**
- Informationssicherheits-Organisation

Informationssicherheits-Managementsystems nicht gewährleistet.

Hilfsmittel

Hilfsmittel	Typ
Informationssicherheits-Leitlinie	Muster
Informationssicherheits-Organisation	Beispiel

Siehe auch: Erläuterungen zu den Hilfsmitteln

SIZ Vorstellung

Motivation zur Informationssicherheit

Produkt Sicherer IT-Betrieb

Prozess ISMS

Dokumentationswerkzeug

Zusammenfassung

Dokumentation per Knopfdruck durch den integrierten SIZ-Werkzeugkasten

- Individuelle Ergebnisse und Umsetzungen werden
  - systematisch aufbereitet
  - in Konzepten und Aktivitäten kontextbezogen eingebunden
  - in verschiedenen Berichten und Übersichten aufbereitet
  - in den Sichten spezifisch den Einzelanforderungen berücksichtigt

- Vorhandenen Dokumentationen können eingebunden werden, um redundante Pflege zu vermeiden

Inhalte werden durch den Anwender **individuell** mit den eigenen Ergebnissen und Umsetzungen **befüllt**

Umsetzung

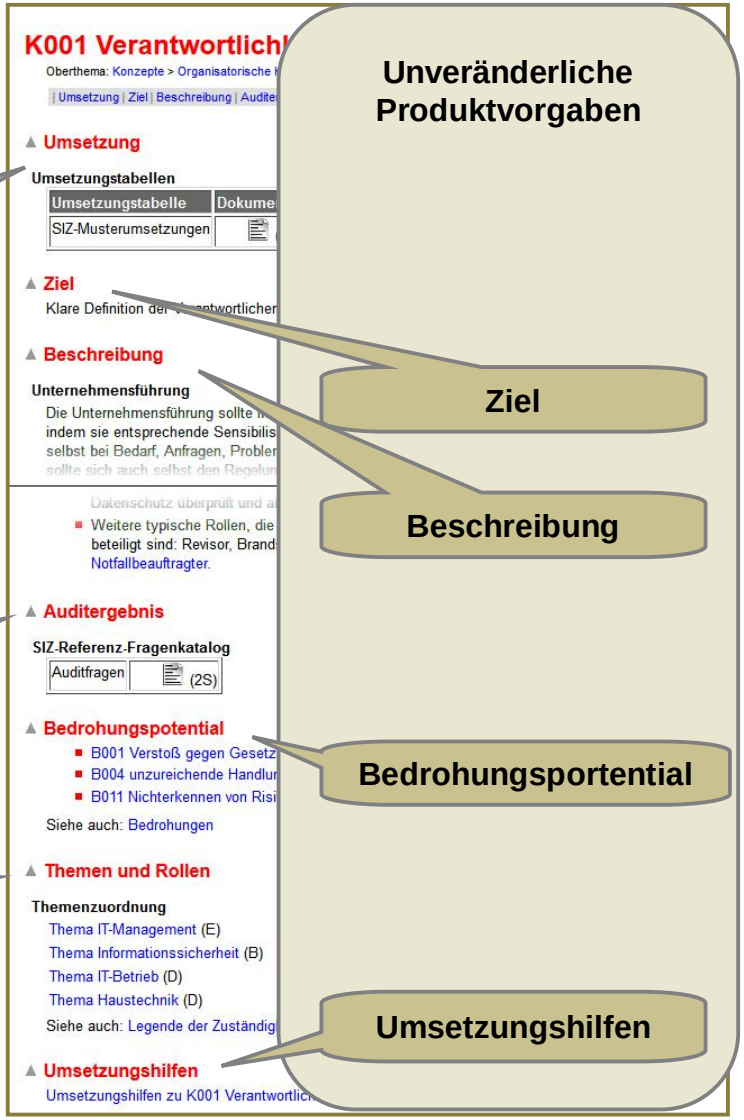
- Arbeitsanweisungen
- Regelungen
- Policies
- Protokolle
- Berichte
- ...

Auditergebnis

- Beantwortete Fragen
- Bewertungen
- Risiken
- Maßnahmen zur Risikobehandlung

Themen und Rollen

- Zuständigkeiten
  Wer ist involviert?
  Wer erfüllt welche Rolle?



Unveränderliche Produktvorgaben

Ziel

Beschreibung

Bedrohungsportential

Umsetzungshilfen

Audit-Ergebnisse werden in verschiedenen Berichten aufbereitet und können bis ins Detail heruntergebrochen werden

Konzepte (Auditübersicht)

Oberthema: Auditergebnis > Audits

Unterthema:
Audit 2010 (Details Konzepte)
Audit 2011 (Details Konzepte)

Siehe auch: Erläuterungen zum Bewertungsschema

	Audit 2010	Audit 2011
K001 Verantwortlichkeiten	7 / 6	8 / 7
K002 Planerische Aufgaben	5 / 5	8 / 8
K003 IS-Risikoanalyse und -behandlung	6 / 5	7 / 5
K004 Informationsaustausch	7 / 7	7 / 7
K005 Berichtswesen	8 / 8	8 / 8
K007 Gesetzliche Anforderungen	8 / 8	8 / 8
K014 Software-Anforderungen	8 / 8	8 / 8
K015 Dokumentations-Anforderungen	8 / 8	8 / 8
K017 Sichere Administration	7 / 7	7 / 7
K018 Trennung der Umgebungen	8 / 8	8 / 8
K020 Archivierung	7 / 7	7 / 7
K021 Übergreifende Regelungen	8 / 8	8 / 8
K024 Schulungen	5 / 5	5 / 5
K025 Sensibilisierung	6 / 6	6 / 6
K026 Versicherungen	7 / 7	7 / 7
K029 Informationsklassifizierung	8 / 8	8 / 8
K030 IS-Gremien	7 / 7	7 / 7
K031 IS-Leitlinie	7 / 7	8 / 8
K032 Inventar der Werte	7 / 7	7 / 7
K033 Personalpolitik	8 / 8	8 / 8

Konzeptkategorien (Auditübersicht)

Oberthema: Auditergebnis > Audits

Unterthema:
Audit 2010 (Details Konzeptkategorien)
Audit 2011 (Details Konzeptkategorien)

Siehe auch: Erläuterungen zum Bewertungsschema

Organisatorische Konzepte

Unterkategorie	Audit 2010	Audit 2011
IS-Organisation	7 / 5	8 / 7
IS-Risikomanagement	7 / 5	8 / 5
Dokumentation, Inventarisierung	8 / 7	8 / 7
Archivierung	7 / 7	7 / 7
Schulung, Sensibilisierung	6 / 5	6 / 5

Logische, technische Konzepte

Unterkategorie	Audit 2010	Audit 2011
Nutzerverwaltung	8 / 8	8 / 8
Schadsoftware, schadhafte Inhalte	8 / 8	8 / 8
Netzstruktur, -sicherheit	8 / 8	8 / 8
Protokollierung, Härtung	8 / 8	8 / 8
Datenaustausch, -ablage	8 / 8	8 / 8
Virtualisierung	8 / 8	8 / 8

Physische Konzepte

Unterkategorie	Audit 2010	Audit 2011
Standort-, Raumfaktoren	8 / 8	8 / 8
Strom, Blitz, Klima	8 / 8	8 / 8
Brandschutz	8 / 8	8 / 8
Zutrittsschutz, Überwachung	8 / 8	8 / 8

Details per Klick

Bewertungen mit **Mittelwert / Minimum**

IS-Risikom…gement (Details K… …011)

Oberth… …dite… …s > Audits > Konzeptkategorien (Auditübersicht)
Organi… …he K… …epte (Details Konzeptkategorien, Audit 2011)

Gesamt…wertung

Gesamtbewertung	Hinweis
8 / 5	Ermittelte Bewertung aus der Gesamtb… Konzepte Siehe auch: Erläuterungen zum Bewer…

Gesamtbewertung der zugehörigen Konzepte

Konzept	Bewertung
K035 IS-Management	8 / 7
K003 IS-Risikoanalyse und -behandlung	7 / 5
K026 Versicherungen	7 / 7
K007 Gesetzliche Anforderungen	8 / 8
K034 Audits	8 / 7

Themen- und Fragendetails

K035 IS-Management: 8 / 7

Frage
F.S.O13.100.GFK (Gesamtfragenkatalog) Ist das ISMS im Sinne eines Prozesses im Unternehmen ve…

Mittels vordefinierter Sichten werden alle Inhalte aus der Perspektive des in der Sicht behandelten Standards aufbereitet

Sicherer IT-Betrieb

Sicht: ISO/IEC 2700x | Start | Stichwortsuche | Versionsinfo | Glossar |

- Sicht ISO/IEC 2700x
- ISO/IEC 27000:2009
- ISO/IEC 27001:2005
- ISO/IEC 27002:2005
- ISO/IEC 27003:2010
- ISO/IEC 27004:2009
- ISO/IEC 27005:2008
- Konzepte
  - Organisatorische Konzepte
  - Logische, technische Konzepte
  - Physische Konzepte
  - Konzepte Notfallbehandlung
  - Betriebskonzepte
  - Konzepte Vertragsbeziehung
  - Konzepte ISMS-Schnittstellen
  - Register der Konzepte
  - Konzeptverlinkung in den Sichten
  - Zugeordnete Auditfragen
- Auditergebnis
  - Erläuterungen zum Bewertungsschema
  - Audits
    - Konzepte (Auditübersicht)
    - Konzeptkategorien (Auditübersicht)
    - ISO 27001 (Auditübersicht)
    - ISO 27001A (Auditübersicht)
    - Audits Quellen
- Prozess Informationssicherheits-Management

ISO 27001A (Auditübersicht)

Oberthema: Auditergebnis > Audits

Unterthema:
Audit 2010 (Details ISO 27001A)
Audit 2011 (Details ISO 27001A)

Siehe auch: Erläuterungen zum Bewertungsschema

	Audit 2010	Audit 2011
A.5.1.1 Dokument zur Informationssicherheitspolitik	7 7	8 8
A.5.1.2 Überarbeitung des Dokuments zur Informationssicherheitspolitik	7 5	8 7
A.6.1.1 Engagement der Geschäftsführung für die Informationssicherheit	7 6	8 7
A.6.1.2 Informationssicherheitskoordination	7 5	8 7
A.6.1.3 Zuweisung der Zuständigkeiten für Informationssicherheit	7 6	8 7
A.6.1.4 Berechtigungsprozess für Informationsverarbeitungseinrichtungen	8 8	8 8
A.6.1.5 Geheimhaltungsvereinbarungen	8 5	8 5
A.6.1.6 Kontakt zu Behörden und amtlichen Stellen	8 8	8 8
A.6.1.7 Kontakte zu Interessenverbänden	8 7	8 7
A.6.1.8 Unabhängige Überprüfung der Informationssicherheit	7 5	8 7
A.6.2.1 Feststellung von Risiken im Zusammenhang mit externen Partnern	8 5	8 5
A.6.2.2 Klärung von Sicherheitsfragen beim Umgang mit Kunden	8 5	8 5
A.6.2.3 Klärung von Sicherheitsfragen in Verträgen mit Dritten	8 5	8 5
A.7.1.1 Inventar der Werte	7 7	7 7
A.7.1.2 Eigentum an Werten	7 7	7 7
A.7.1.3 Akzeptable Verwendung von Werten	8 8	8 8
A.7.2.1 Klassifizierungsrichtlinien	8 8	8 8
A.7.2.2 Kennzeichnung und Behandlung von Informationen	8 8	8 8

Details per Klick

Gesamtbewertung

Gesamtbewertung	Hinweis
7 5	Ermittelte Bewertung a Siehe auch: Erläuterun

Gesamtbewertung der zugehörigen K

Konzept	Bewertung
K002 Planerische Aufgaben	5 5
K004 Informationsaustausch	7 7
K031 IS-Leitlinie	7 7
K034 Audits	8 7

Bewertungen mit **Mittelwert / Minimum**

SIZ Vorstellung

Motivation zur Informationssicherheit

Produkt Sicherer IT-Betrieb

Prozess ISMS

Dokumentationswerkzeug

Zusammenfassung

Zusammenfassung

- Das Produkt Sicherer IT-Betrieb stellt
  - einen ganzheitlicher Ansatz zum Informationssicherheits- und IT-Risikomanagement dar, mit
  - vollständiger Abdeckung des Lebenszyklus der Informationssicherheit und des IT-Betriebs.
- Dabei handelt sich um einen risikoorientierter Ansatz für wirtschaftlich sinnvolle und angemessene Lösungen
- Alle Ebenen im Unternehmen, von der Geschäftsführung bis zum Nutzer und Techniker werden adressiert.
- Harmoniert mit gängigen Standards z.B. ISO/IEC 27001:2005

Vielen Dank für Ihre Aufmerksamkeit

INFORMATIKZENTRUM DER SPARKASSEN-ORGANISATION GMBH

INFORMATIKZENTRUM DER SPARKASSEN-ORGANISATION GMBH

Dr. Detlef Reich

Simrockstr. 4

53113 Bonn

Telefon: +49 (228) 4495 7 322

Telefax: +49 (228) 4495 7 555

E-Mail:

Detlef.Reich@SIZ.de

Internet:
http://www.siz.de