Aufwand und Nutzen der BSI-Zertifizierung aus Sicht eines zertifizierten Unternehmens

Fachgruppe Management von Informationssicherheit

7. Juni 2013

Klaus Foitzick
Vorstand activeMind AG

Geschäftsführer Global Access Internet Services GmbH

Agenda

activeMind AG

- Kurzvorstellung activeMind AG
- Vorstellung Global Access Internet Services GmbH
- Bestehende Grundlagen im Unternehmen
- Gründe für den Zertifizierungswunsch
- Planung und Umsetzungsschritte
- Herausforderungen bei der Umsetzung
- Zertifizierungsaudit
- Reaktion der Kunden und Interessenten
- Resümee

Kurzvorstellung activeMind AG

activeMind · AG

Gründung 2000

Mitarbeiter

- 3 Rechtsanwälte, 3 ISO 27001 Auditoren (TÜV), 2 BSI Auditoren, 1 ISO 9001 Auditor (TÜV), 1 ULD Prüfstellenleiter (Recht und Technik), 1 VCP, 1 MCSE, 2 ITIL Foundation Manager

Unternehmensschwerpunkte

- Externe Datenschutzbeauftragte bundesweit
- Vorbereitung und Auditierung ISO 27001 / BSI / ISO 9001

Besonderheiten

- Hohe technische Fachkompetenz
- Abrechnung zu monatlichen Pauschalen mit garantierter SLA im Bereich Datenschutz, ISO 27001, BSI, ISO 9001

Aufgabe der activeMind AG

activeMind erhielt Mitte 2012 die Aufgabe Global Access bis Ende 2012 durch die BSI Zertifizierung zu führen

- Stellung des Sicherheitsbeauftragten
- Strukturanalyse / Modellierung / Befüllung GS-Tool
- Schulung der Mitarbeiter
- Durchführung interne Audits / Basissicherheitscheck / Risikoanalyse
- Projektplanung und Projektsteuerung
- Entwicklung und Erweiterung der Dokumentationsstruktur
- Erweiterung der bestehenden Regelungsdokumente
- Technische Unterstützung bei der Umsetzung in Bereichen wie: MS-Infrastruktur, Virtualisierung…

Vorstellung

Global Access Internet Services GmbH

Leistungen

Global Access stellt seinen Kunden seit mehr als 18 Jahren folgende Kernleistungen zur Verfügung:

- Rechenzentrum (Colocation und managed Colocation)
- Private Cloud Services (milkcloud.com)
- Internet Services (Anbindung und CDN)
- Security-as-a-Service (AV, FW, IPS, Verschlüsselung…)

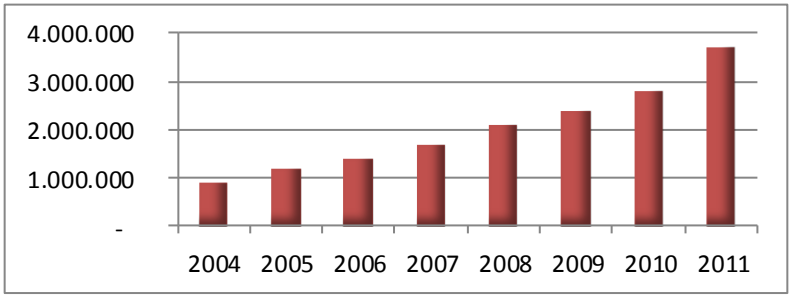
Entwicklung

1996	Gründung als ISP
2000	Aufbau Datacenter Services
2002	Bundesweite RZ-Leistungen
2003	Einführung WAN Services
2005	Papierloses Büro
2006	Vollständige Virtualisierung der ISP-Umgebung
2007	Zertifizierung nach ISO 9001 & ISO/IEC 27001
2008	Cloud Services
2009	Datacenter Redundanz
2013	ISO 27001 a.B. IT-GS

Zahlen

6.400	TerraByte Traffic pro Monat
474	Leitungen in MPLS-Netzen von DSL bis 10 Gbit/s-Ethernet
143	Multi-Service-Kunden
134	19“-Schränke mit Kundenservices
44	Gbit/s Bandbreite für Internetanbindung
8	Rechenzentren
3	Zertifizierungen

98% unseres Umsatzes sind Serviceleistungen!



8

Bestehende Grundlagen im Unternehmen

TÜV PROFI CERT

ZERTIFIKAT

für das Managementsystem nach

DIN EN ISO 9001:2008

Der Nachweis der regelkonformen Anwendung wurde erbracht und wird gemäß TÜV PROFICERT-Verfahren bescheinigt für

GLOBAL ACCESS

Global Access Internet Services GmbH
Wamslerstraße 8, D-81829 München
Elisabeth-Selbert-Straße 7, D-80939 München

Geltungsbereich

Betrieb der folgender Leistungen:
Datacenter, Security as a Service, Internet Services und VMware Hosting im Rahmen der milkcloud.com

Zertifikat-Registrier-Nr.	73 100 4026-4
Auditbericht-Nr.	4252 1279
Zertifikat gültig bis	2015-09-30

TGA-ZM-0547-00

TÜV HESSEN

Darmstadt, 2012-10-01
Zertifizierungsstelle des TÜV Hessen
- Der Zertifizierungsstellenleiter -

SEITE 2. Nur gültig in Verbindung mit dem Hauptzertifikat.
Diese Zertifizierung wurde gemäß TÜV PROFICERT-Verfahren durchgeführt und wird regelmäßig überwacht.
Die aktuelle Gültigkeit ist nachprüfbar unter www.tuev-club.de. Originalzertifikate enthalten ein aufgeklebtes Hologramm.
TÜV Technische Überwachung Hessen GmbH, Rüdesheimerstr. 119, D-64285 Darmstadt, Tel. +49 6151/600331

TÜV PROFI CERT

ZERTIFIKAT

für das Managementsystem nach

DIN ISO/IEC 27001:2008

Der Nachweis der regelkonformen Anwendung wurde erbracht und wird gemäß TÜV PROFICERT-Verfahren bescheinigt für

GLOBAL ACCESS

Internet Services GmbH
Wamslerstraße 8, D-81829 München
Elisabeth-Selbert-Straße 7, D-80939 München

Geltungsbereich

Betrieb folgender Leistungen:
Hosting virtueller Infrastrukturen (milkcloud.com), Security as a Service, MPLS VPN, Internet Services sowie umfassende Datacenter Leistungen.

Anwendbarkeitserklärung (SoA): 2012-07-02

Zertifikat-Registrier-Nr.	73 121 4126
Auditbericht-Nr.	4255 7530
Zertifikat gültig bis	2014-01-13

DAkkS Deutsche Akkreditierungsstelle D-ZM-14137-01-01

TÜV HESSEN

Darmstadt, 2013-01-24
Zertifizierungsstelle des TÜV Hessen
- Der Zertifizierungsstellenleiter -

SEITE 1 VON 1
Diese Zertifizierung wurde gemäß TÜV PROFICERT-Verfahren durchgeführt und wird regelmäßig überwacht.
Die aktuelle Gültigkeit ist nachprüfbar unter www.tuev-club.de. Originalzertifikate enthalten ein aufgeklebtes Hologramm.
TÜV Technische Überwachung Hessen GmbH, Rüdesheimerstr. 119, D-64285 Darmstadt, Tel. +49 6151/600331

Gründe für den Zertifizierungswunsch

- Verstärkte Nachfragen aus dem Kundenbereich
  - Versicherungen
  - Öffentliche Auftraggeber
- In Ausschreibungen verstärkt BSI gefordert
- Erster Anbieter von Cloudleistungen mit BSI Zertifizierung
- Wunsch nach höherer Transparenz im Bereich der technischen Umsetzung
- Technischer Anspruch und Herausforderung

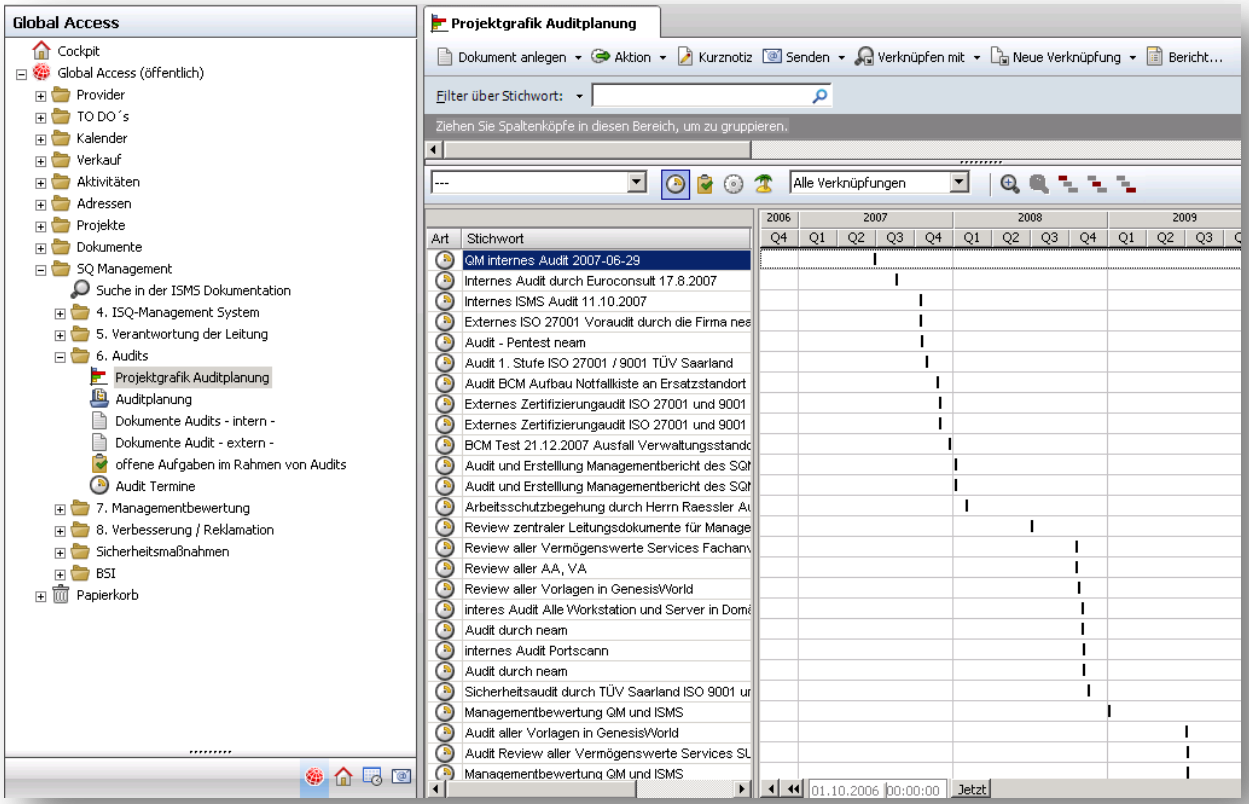
Planung und Umsetzungsschritte

2012	Tätigkeitsschritte
Juli	Strukturanalyse / Modellierung
August	Befüllung GS-Tool / Schulung der Mitarbeiter
September	Durchführung interne Audits / Basissicherheitscheck / Risikoanalyse
Oktober	• Erweiterung der bestehenden Regelungsdokumente • Aufbau eines gemeinsamen Dokumentenrahmens für die Normen ISO 9001 / 27001 / BSI • technische Umsetzung der GS-Katalog Anforderungen
November	technische Umsetzung der GS-Katalog Anforderungen
Dezember	Erstellung Referenzdokumente / Auditvorbereitung / Kombiaudit ISO 27001 nativ und ISO 27001 a.B. IT-Grundschutz
Januar	Abschluss Vor-Ort-Audit / Auditbericht durch Auditor an das BSI

Exemplarische Herausforderung:

Planung, Steuerung und Dokumentation des Projektes

Detaillierte Projektplanung im DMS



Über 300 Einzeltermine zu koordinieren

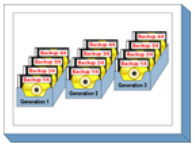
Exemplarische Herausforderung:

Vorbereitung und Durchführung des Basissicherheitschecks

Aufbereiten des Fragenkataloges I

IT-Grundschutzerhebung: Formular zu Baustein B 1.4 Datensicherungskonzept

Nummer des IT-Systems: _____ Erfasst am: _____ Befragte Personen _____
Bezeichnung: _____ Erfasst durch: _____ - " - _____
Standort _____ - " - _____
- " - _____
- " - _____



Maßnahme (Priorität)	Baustein B 1.4 Datensicherungskonzept	entbehrlich	Ja	teilweise	Nein	Umsetzung bis	verantwortlich	Bemerkungen / Begründung für Nicht-Umsetzung	Kostenschätzung
M 2.41 (2) [A]	Verpflichtung der Mitarbeiter zur Datensicherung								
M 2.137 (2) [A]	Beschaffung eines geeigneten Datensicherungssystems								
M 6.20 (1) [A]	Geeignete Aufbewahrung der Backup-Datenträger								
M 6.21 (1) [C]	Sicherungskopie der eingesetzten Software								
M 6.22 (1) [A]	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen								
M 6.32 (1) [A]	Regelmäßige Datensicherung								
M 6.33 (2) [B]	Entwicklung eines Datensicherungskonzepts								

Aufbereiten des Fragenkataloges II

B 1.4 Datensicherungskonzept

Verbundenes Prüfobjekt:			
Tag der Befragung:		**Prüfer:**	
Ort der Befragung:			
Befragte Personen:			

Votum: ja, teilweise, nein, entbehrlich
schwerwiegend / geringfügig

Was ist zu prüfen?	Prüffragen	Prüfungsergebnis	Bewertung
Planung und Konzeption			
M 6.33 (B) - Entwicklung eines Datensicherungskonzepts	▪ Ist für die Institution ein aktuelles Datensicherungskonzept dokumentiert? ▪ Sind sämtliche betroffenen IT-Systeme in diesem Konzept aufgeführt? ▪ Wie werden Mitarbeiter über den sie betreffenden Teil des Konzepts unterrichtet? ▪ Wird die Einhaltung dieses Konzepts kontrolliert? ▪ Wie werden Änderungen der Einflussfaktoren berücksichtigt?	▪	
M 6.34 (B) - Erhebung der Einflussfaktoren der Datensicherung	▪ Wurden bei der Erhebung der Einflussfaktoren sowohl die Systemadministratoren als auch die IT-Anwender eingebunden? ▪ Wie werden diese Angaben aktualisiert? ▪ Werden neue Anforderungen rechtzeitig in einem aktuali-	▪	

Baustein B 1.4 Datensicherungskonzept (Beispiel).Docx
Stand: 06.06.2012

Seite 1 von 4

Vermittlung der Beantwortungstiefe und Detaillierung Beispielantwort:

- **Es besteht ein aktuelles Datensicherungskonzept im Portal. (Version 15)**
- **Die betroffenen IT-Systeme sind derzeit innerhalb des Datensicherungskonzepts nicht genannt.**
- **Die Mitarbeiter werden im Rahmen der Schulung auf die Notwendigkeit der Datensicherung hingewiesen. (nicht in Schulungsunterlagen dokumentiert)**
- **Soweit möglich erfolgen die Datensicherungen automatisiert. Lokale Systeme der Mitarbeiter müssen nicht gesichert werden, da sich hierauf keine sensiblen Daten befinden. Bei Problemen mit den jeweiligen Stationen wird diese auf Basis eines Images neu installiert.**
- **Veränderungen an Systemen erfolgen im Rahmen des Change Verfahrens. Im Rahmen dessen wird auch der Bedarf von Datensicherungsverfahren geprüft und ggf. eingeleitet.**

Umsetzungsstatus:

teilweise

Dokumentation der Ergebnisse des BSC

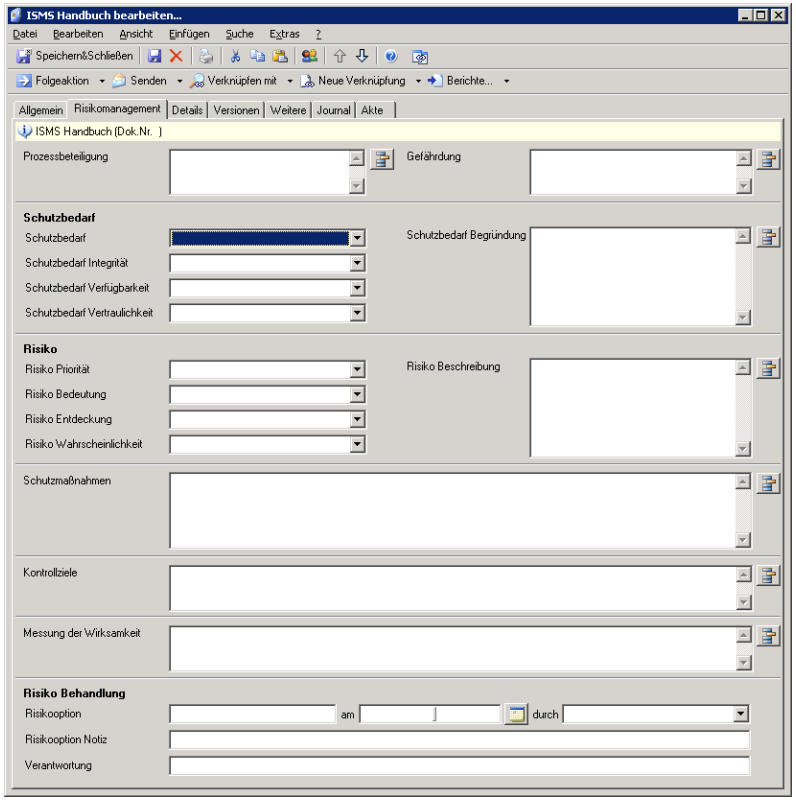
	A	B	C	D	E	F	G	H	I
1	Baustein	Was ist zu prüfen?	Prüffragen	Prüfungsergebnis	Status	to DO	Aufwandsschätzung	fertigstellen bis	Verantwortlich
1005	B 2.9 Rechenzentrum Wamsler 8	M 1.3 (A) – Angepasste Aufteilung der Stromkreise	Wird regelmäßig überprüft, ob die Absicherung und Auslegung der Stromkreise noch den tatsächlichen Bedürfnissen genügen?	Belastung aller Suites wird monatlich anhand der Rechnung des Lieferanten und der eigenen Dokumentation (siehe nächster Punkt) verglichen. Im Rahmen der monatlichen Auslastung der Stromlast (NZR eigenes System) wird dazu die maximale Last in der Datei Verbrauchswerte festgehalten. Der Vertrag mit den Lieferanten sieht vor, die Maximallast von Strom und Kühlung automatisch der tatsächlichen Last anzupassen.	korrekt				Manfred
1006	B 2.9 Rechenzentrum Wamsler 8	M 1.3 (A) – Angepasste Aufteilung der Stromkreise	Wann erfolgte die letzte Bestandsaufnahme des Leistungsbedarfs im Raum?	Die letzte Überprüfung erfolgte zum Anfang des aktuellen Monats (für den Vormonat)	korrekt				Manfred
1007	B 2.9 Rechenzentrum Wamsler 8	M 1.7 (A) – Handfeuerlöscher	Gibt es an allen notwendigen Stellen eine ausreichende Zahl geeigneter Handfeuerlöscher?	Es gibt eine ausreichende Anzahl von Feuerlöschern in den IT Räumen	korrekt				Manfred
1008	B 2.9 Rechenzentrum Wamsler 8	M 1.7 (A) – Handfeuerlöscher	Sind die Mitarbeiter über die Aufbewahrungsorte der Handfeuerlöscher informiert?	Die Mitarbeiter sind momentan nicht darüber geschult, wo sich die Handfeuerlöscher befinden àKlären	Frage				Manfred
1009	B 2.9 Rechenzentrum Wamsler 8	M 1.7 (A) – Handfeuerlöscher	Ist sichergestellt, dass in der Nähe von IT-Räumen keine Pulverlöscher bereitgestellt werden oder diese zumindest so aufbewahrt werden, dass sie in der Aufregung eines Brandes nicht versehentlich verwendet werden?	Es werden keine Pulverhandfeuerlöscher eingesetzt	korrekt				Manfred
1010	B 2.9 Rechenzentrum Wamsler 8	M 1.7 (A) – Handfeuerlöscher	Wird die Nutzung der Handfeuerlöscher geübt?	Die Nutzung der Handfeuerlöscher wird nicht geübt	Frage				Manfred
1011	B 2.9 Rechenzentrum Wamsler 8	M 1.7 (A) – Handfeuerlöscher	Werden die Handfeuerlöscher regelmäßig inspiziert und gewartet?	Die Handfeuerlöscher werden regelmäßig durch die RZ Betreiber inspiziert und gewartet	korrekt				Manfred
1012	B 2.9 Rechenzentrum Wamsler 8	M 1.10 (C) – Verwendung von Sicherheitstüren und -fenstern	Wurde untersucht, wo Sicherheitstüren und -fenster sinnvollerweise eingebaut werden sollten?	Ja, vom Gebäudebetreiber selbst. Es gibt keine Fenster zu den RZ Räumen. Türen sind alle Sicherheitstüren, sowohl gegen Brand wie auch unbefugten Zutritt	korrekt				Manfred

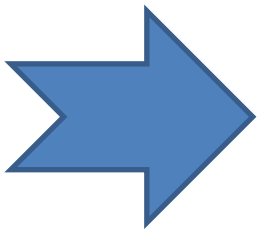
8734 zu bewertende Einzelmaßnahmen knapp 1500 nicht vollständig umgesetzt (September 2012)

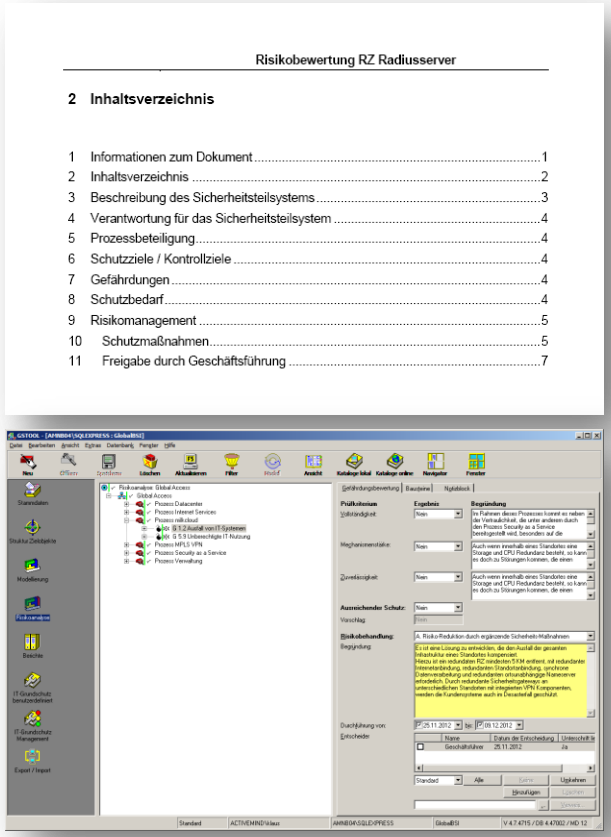
Exemplarische Herausforderung:

Gemeinsame Risikoanalyse für ISO 27001 und BSI mit ähnlichen Ergebnissen

Risikoanalyse für ISO 27001 nativ und BSI







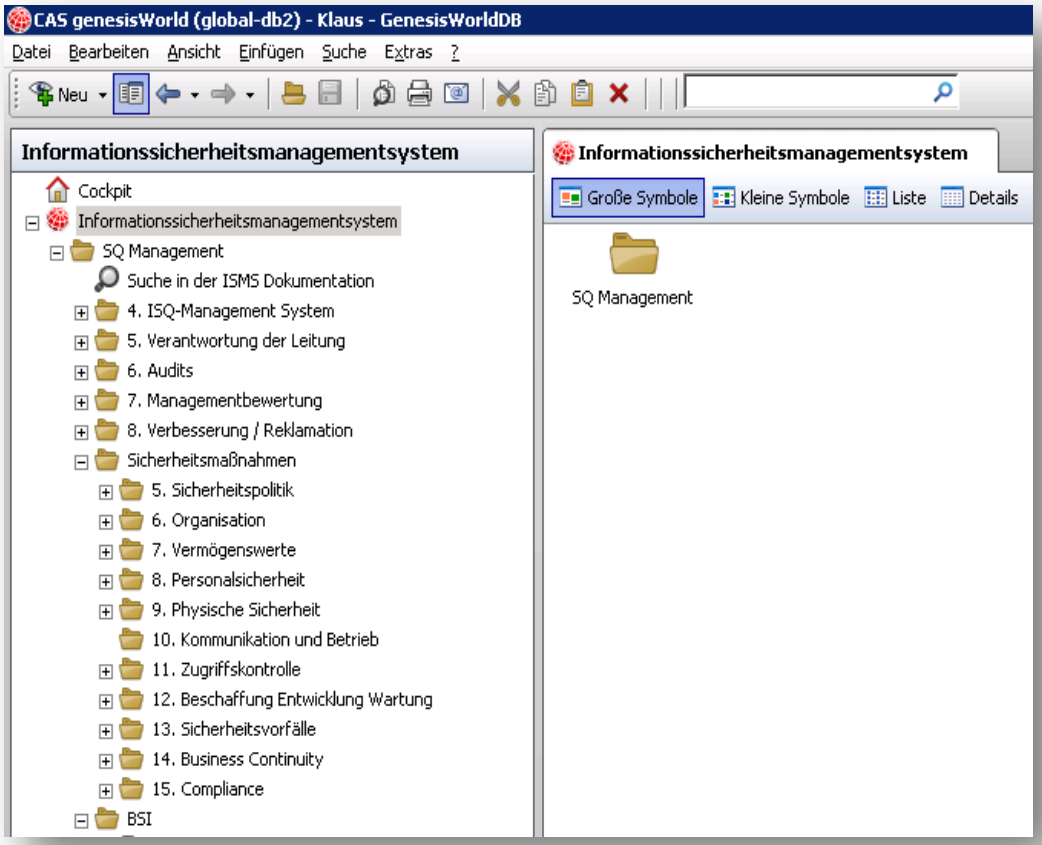
Risikobewertung RZ Radiusserver

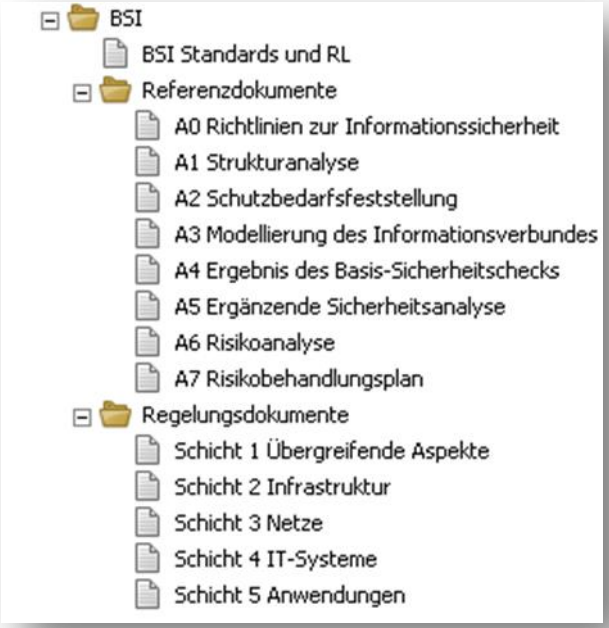
2 Inhaltsverzeichnis

Exemplarische Herausforderung:

Aufbau eines gemeinsamen Dokumentenrahmens für die Normen ISO 9001 / ISO 27001 / BSI

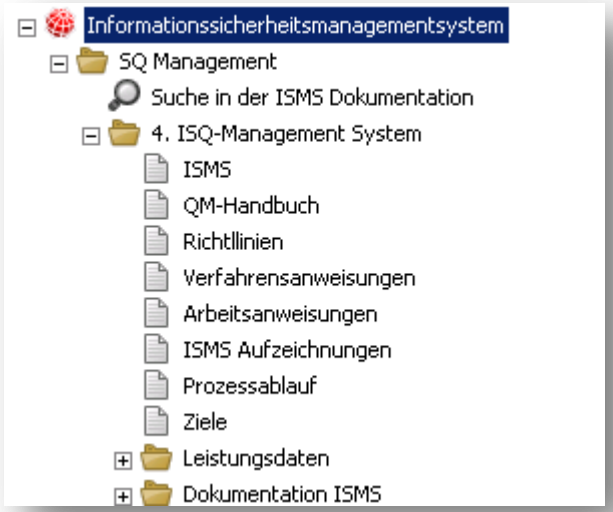
Dokumentenrahmen im DMS

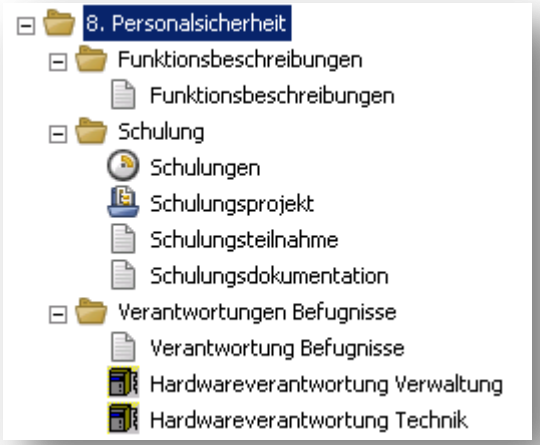


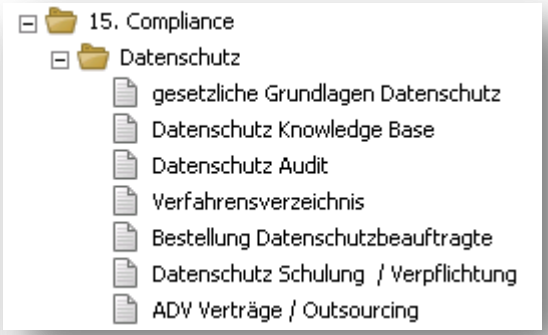


Über 150 Regelungsdokumente
Problem: Vermeidung von Redundanzen

Auszüge des Dokumentenrahmens







Im DMS werden auch alle Aufzeichungen archiviert und versioniert.

Zertifizierungsaudit

- Kombiaudit ISO 27001 nativ und ISO 27001 a.B. IT-Grundschutz
- Zwei Rechenzentren
- 7 Audittage vor Ort
- 1 Geringfügige Abweichung

…und dann endlich

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat
erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-IGZ-0143-2013

ISO 27001-Zertifikat auf der Basis von IT-Grundschutz

Betrieb der Leistungen: Virtual Server, Security as a Service, Datacenter, MPLS VPN Internet Access

der Global Access Internet Services GmbH

gültig bis: 5. März 2016*

Die Global Access Internet Services GmbH (global.de) betreibt mehrere Rechenzentren im Gebiet der Bundesrepublik Deutschland und bietet Hosting virtueller Infrastrukturen (milkcloud.com), Security as a Service, MPLS VPN, Internet Access sowie umfassende Colocationsleistungen an. Der Geltungsbereich des ISMS beschränkt sich auf das Rechenzentrum der Global Access Internet Services GmbH in München Ost, sowie den Rechenzentrumsstandort München Nord. Einbezogen sind alle die IT-Sicherheit betreffenden Aspekte in Bezug auf Organisation, Personal und Technik. In den Geltungsbereich technisch eingeschlossen sind alle Übergabepunkte und internen Systeme, die für die Verwaltung der Firma Global Access und deren Services für die Kunden einsetzt werden. Begleitend zu den technischen Komponenten zählt die Betrachtung der infrastrukturellen, organisatorischen und personellen Sicherungsmaßnahmen. Das Hosting virtueller Infrastrukturen erfolgt ausschließlich an den beiden Standorten im Geltungsbereich.

Der oben aufgeführte Untersuchungsgegenstand wurde von Peter Pakosch, zertifizierter Auditor für ISO 27001-Audits auf der Basis von IT-Grundschutz, in Übereinstimmung mit dem Zertifizierungsschema des Bundesamtes für Sicherheit in der Informationstechnik geprüft. Die im Auditbericht enthaltenen Schlussfolgerungen des Auditors sind im Einklang mit den erbrachten Nachweisen.

Die durch dieses Zertifikat bestätigte Anwendung von ISO 27001 auf der Basis von IT-Grundschutz umfasst die Maßnahmenziele und Maßnahmen aus Annex A von ISO/IEC 27001 und die damit verbundenen Ratschläge zur Umsetzung und Anleitungen für allgemein anerkannte Verfahren aus ISO/IEC 27002. Dieses Zertifikat ist keine generelle Empfehlung des Untersuchungsgegenstandes durch das Bundesamt für Sicherheit in der Informationstechnik. Eine Gewährleistung für den Untersuchungsgegenstand durch das Bundesamt für Sicherheit in der Informationstechnik ist weder enthalten noch zum Ausdruck gebracht.

Dieses Zertifikat gilt nur für den angegebenen Untersuchungsgegenstand und nur in Zusammenhang mit dem vollständigen Zertifizierungsreport.

Bonn, 6. März 2013
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag
Joachim Weber
Fachbereichsleiter

* Unter der Bedingung, dass die ab 6. März 2013 jährlich durchzuführenden Überwachungsaudits mit positivem Ergebnis abgeschlossen werden.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon +49 (0)228 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 9582-111

Aufwand Vorbereitung und Zertifizierungsaudit

Tätigkeitsschritte	activeMind AG	Global Access GmbH
Strukturanalyse / Modellierung	5 Tage	2 Tage
Befüllung GS-Tool / Schulung der Mitarbeiter	5 Tage	3 Tage
Durchführung interne Audits / Basissicherheitscheck / Risikoanalyse	20 Tage	15 Tage
• Erweiterung Regelungsdokumente • Aufbau Dokumentenrahmens • technische Umsetzung	18 Tage 2 Tage 5 Tage	5 Tage 0 Tage 20 Tage
• technische Umsetzung	5 Tage	35 Tage
Erstellung Referenzdokumente / Auditvorbereitung / Audit / Nacharbeiten	15 Tage	10 Tage

Kosten Vorbereitung und 3 Jahre Betrieb

Kostenblock	activeMind AG	Global Access GmbH
Externe Beratung Rahmenvertrag für 36 Monate Vorbereitung / interne Audits / Auditbegleitung	3.000 € monatlich damit 108.000 €	
Interne Personalkosten		60.000 €
Kosten BSI	2.500 €	
Kosten Auditor	20.000 €	
Kosten anzuschaffende Technologie		15.000 €
Kosten externe IT-Dienstleister	35.000 €	

Gesamtkosten für 3 Jahre ca. 250.000 €

Reaktion der Kunden und Interessenten

- 5 Mails mit „Glückwünschen“
- 2 neue größere Anfragen mit „BSI-Bezug“
- Verwendung in einer Ausschreibung

Kein unmittelbarer finanzieller Return of Invest

Weitere Kundenbindung / Langfristige Verbesserung Wettbewerbssituation

Resümee

- BSI Zertifizierung schafft primär keine neuen Kunden, sondern hält Kunden
- Return of Security Investment nur mittelfristig
- Deutliche Verbesserung der technischen Transparenz
- Deutlicher Erhöhung der Regelungstiefe und damit Erhöhung der Personenunabhängigkeit
- Erhöhung des Firmenwertes
- Wir würden es wieder machen…

Gibt es Fragen?

Vielen Dank für die Aufmerksamkeit

Kontaktdaten

Klaus Foitzick
Vorstand

activeMind AG
Management und Technologieberatung

Potsdamer Straße 3
80802 München
Tel: +49 89 418 56 01 - 70
Fax: +49 89 418 56 01 - 79
Web: www.activemind.de
E-Mail: foitzick@activemind.de

- **Volljurist**
- **MCSE, VCP, ITIL v3 Manager**
- **ISO 9001 / 27001 Auditor des TÜV**
- **Auditorteamleiter der Bundesamtes für Sicherheit in der Informationstechnik (BSI) ISO 27001 auf Basis IT Grundschutz.**
- **Akkreditierter Prüfstellenleiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD)**