SerNet

Best of Audit 2012
„IT-Sicherheit? Evaluieren wir gerade.“

28. Februar 2013

Alexander Koderman

SerNet GmbH, Berlin

Übersicht

SerNet

- Wieso werde ich auditiert?
  - IS-Audits, Grundlagen, Standards
- Was erwartet mich?
  - Inhalte, Prüftiefe, Vorgehensweisen
- Was muss ich tun?
  - Vorbereitung, Begleitung, Reaktion

SerNet GmbH

SerNet

- gegründet 1997
- Büros in Göttingen und Berlin
- Themen: Informationssicherheit und Datenschutz
- spezialisiert auf Open Source Software
- verinice.: Open Source ISMS Tool
- SAMBA: Windows/Linux-Interoperabilität, Clustering und Private Clouds
- Zertifizierungen und Audits, IT-Grundschutz und ISO 27001
- Firewalls und VPN-Lösungen für mittlere und große Einrichtungen
- Old Economy: kein Risiko-Kapital, keine Bank-Kredite
- über 1500 Bestandskunden in DE, EU, US

Übersicht

SerNet

- Wieso werde ich auditiert?
  - IS-Audits, Grundlagen, Standards
- Was erwartet mich?
  - Inhalte, Prüftiefe, Vorgehensweisen
- Was muss ich tun?
  - Vorbereitung, Begleitung, Reaktion

IS-Audits

SerNet

- ...durch Kunden
- ...durch Wirtschaftsprüfer
- ...durch Prüfungsstellen

IS-Audits durch Kunden

SerNet

- durch den DSB
- BDSG §9: Technische und organisatorische Maßnahmen
- BDSG §11:
  - Abs. 2 Dienstleister ist unter Prüfung der vorhandenen TOMs sorgfältig auszuwählen
  - Auftrag schriftlich zu erteilen
  - Abs. 7 Kontrollrechte und Mitwirkungspflicht

IS-Audits durch Kunden

SerNet

- „[...] sichert der Auftragnehmer dem Auftraggeber zu, alle Maßnahmen zu treffen, die [...] gemäß der Anlage zu § 9 BDSG[...]erforderlich sind. Diese derzeit erforderlichen Maßnahmen sind in Anhang A beschrieben.“

- „Auf Wunsch stellt der Auftragnehmer dem Auftraggeber ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsdatenverarbeitung nach dieser Vereinbarung zur Verfügung.“

- „Übergabe sämtlicher Angaben gem §4g Abs 2“

IS-Audits durch Kunden

SerNet

- „Der Auftraggeber kann **jederzeit und unverzüglich die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarung durch den Auftragnehmer, auch in dessen Betriebsstätten, kontrollieren,** insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme beim Auftragnehmer. Er darf das Ergebnis der Kontrollen dokumentieren. Der Auftraggeber kann die Kontrollen selbst durchführen oder durch einen beauftragten Dritten durchführen lassen. **Der Auftragnehmer ist entsprechend zur Auskunft und Mitwirkung verpflichtet.“**

IS-Audits durch Kunden

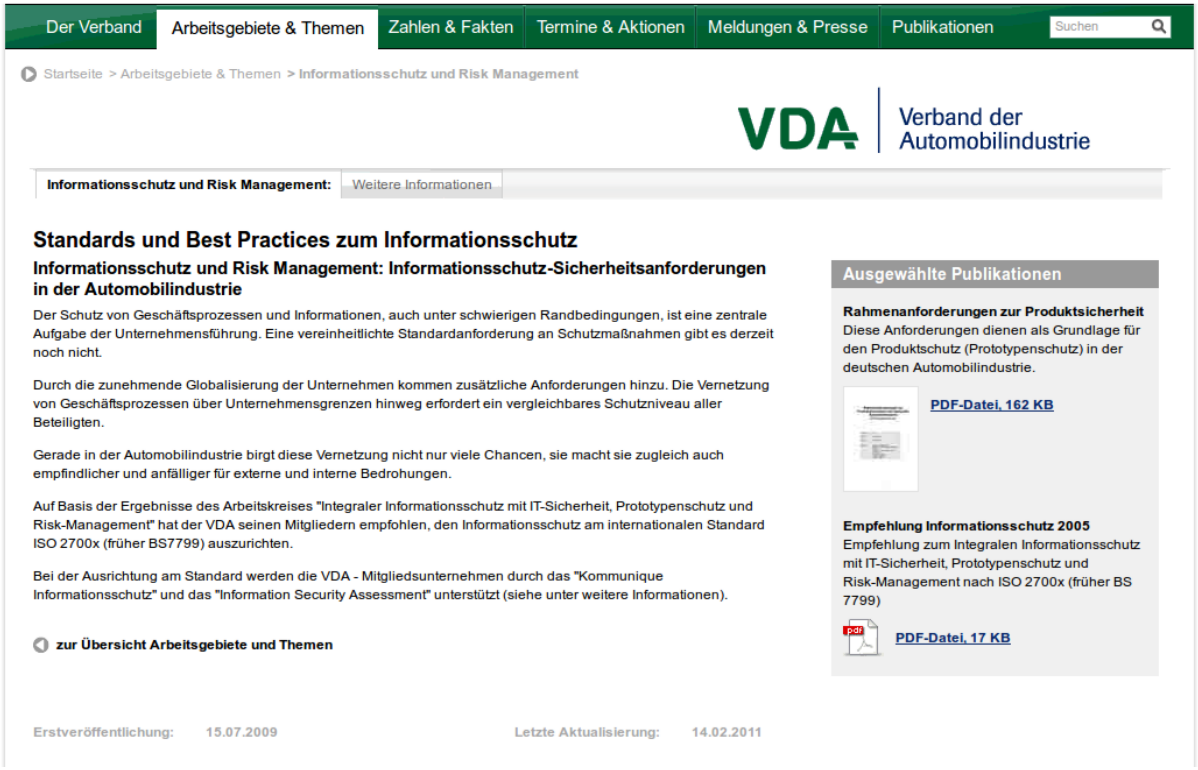
SerNet

- Unterauftragnehmer
  - Der Auftragnehmer stellt sicher, dass der Subunternehmer gegenüber dem Auftragnehmer **in entsprechender Weise** verpflichtet ist, wie der Auftragnehmer gegenüber dem Auftraggeber nach dieser Vereinbarung verpflichtet ist.
  - Der **Auftragnehmer** hat die Einhaltung dieser Pflichten des Subunternehmers, insbesondere die Einhaltung der dort vereinbarten technischen und organisatorischen Maßnahmen, **vor Beginn der Datenverarbeitung und sodann regelmäßig zu überprüfen.** Das Ergebnis ist zu dokumentieren.

IS-Audits durch Kunden

SerNet

- VDA ISA



IS-Audits durch Wirtschaftsprüfer

SerNet

- **§322, §317, §321 HGB**
  - fordert Prüfungsaussagen über die Ordnungsmäßigkeit der Buchführung (Kriterien s. §316, §267 HGB)
- **IDW PS 330: Abschlussprüfung bei Einsatz von Informationstechnologie**
- **seit 2001, ersetzt FAMA 1/1987**

IS-Audits durch Wirtschaftsprüfer

SerNet

- FAIT 1
  - Grundsätze ordnungsgemäßer Buchführung beim Einsatz von IT
  - Ordnungsmäßigkeits *und* *Sicherheitsanforderungen*

IS-Audits durch Prüfungsstellen

SerNet

- ISO 2700x
- BSI IT-Grundschutz
- …

MFG

SerNet

- ISO 27001 / 27002, 27005, ISO 27011, BSI IT-Grundschutz, AktG, GmbHG, BDSG, TMG, IDW PS 330 / FAIT 1 / PS 9.330.1, VDA ISA, CoBIT, COSO, PCI DSS, AICPA SAS 94, SEC 17 CFR, FFIEC IT Exams, HIPAA, CTPAT, EU Direktive 2002/58/EC, 95/46/EC, PAS 77, BS 25999, ISO 20000, OECD World Bank Tech. Risk Checklist...

Übersicht

SerNet

- Wieso werde ich auditiert?
  - IS-Audits, Grundlagen, Standards
- Was erwartet mich?
  - Inhalte, Prüftiefe, Vorgehensweisen
- Was muss ich tun?
  - Vorbereitung, Begleitung, Reaktion

Datenschutzprüfung

SerNet

- Vorhandensein des Datenschutzbeauftragten...
- BDSG §4e: Vorhandensein von Verfahrensangaben, Sicherheitskonzepten
- BDSG §4g: zugriffsberechtigte Personen

Datenschutzprüfung

SerNet

- TOM-Audit
  - Zutrittskontrolle
  - Zugangskontrolle
  - Zugriffskontrolle
  - Weitergabekontrolle
  - Eingabekontrolle
  - Auftragskontrolle
  - Verfügbarkeitskontrolle
  - Verwendungszweckkontrolle
  - weitere (TMG, §88 TKG, durchgeführte Schulungen...)
  - Verträge

Datenschutzprüfung

SerNet

	Die Forderung wurde mit folgenden Maßnahmen erfüllt:	
	a Der Umfang der Berechtigungen, ist auf das zur jeweiligen Aufgaben- bzw. Funktionserfüllung notwendige Minimum zu beschränkt (logisch, zeitlich, ...)	nein
	Die Forderung wurde mit der folgenden alternativen/ergänzenden Maßnahme erfüllt:	nein
	z	
3.1.4	Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen	nein
	Die Forderung wurde mit folgenden Maßnahmen erfüllt:	
	a Ein Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Zugriffsberechtigungen und deren Prüfung ist implementiert.	nein
	b Berechtigungen sind an eine persönliche Benutzerkennung und an einen Account geknüpft	nein
	c Entfällt die Grundlage für eine Berechtigung (z.B. Funktionsänderung) wird diese sofort entzogen	nein
	d Der Prozess wird dokumentiert und die Dokumenation wird 12 Monate aufbewart.	nein
	Die Forderung wurde mit der folgenden alternativen/ergänzenden Maßnahme erfüllt:	nein
	z	
3.1.5	Vermeidung der Konzentration von Funktionen	nein
	Die Forderung wurde mit folgenden Maßnahmen erfüllt:	
	a Es wurde durch geeignete Maßnahmen verhindert, dass durch Konzentration von verschiedenen Rollen bzw. Zugriffsrechten auf eine Person diese in der Kombination eine übermächtige Gesamtrolle erhalten kann.	nein
	Die Forderung wurde mit der folgenden alternativen/ergänzenden Maßnahme erfüllt:	nein
	z	
3.1.6	Protokollierung des Datenzugriffs	nein
	Die Forderung wurde mit folgenden Maßnahmen erfüllt:	
	a Alle Lese-, Eingabe-, Änderungs- und Löschtransaktionen werden protokolliert (Benutzerkennung, Transaktionsdetails) und für mindestens 6 Monate revisionssicher archiviert	nein
	b Zur Missbrauchserkennung werden regelmäßig stichprobenartige Auswertungen vorgenommen	nein
	Die Forderung wurde mit der folgenden alternativen/ergänzenden Maßnahme erfüllt:	nein

- Daten, die direkt in IT-gestützte Rechnungslegung einfließen
- Daten, die als Grundlage für Buchungen zur Verfügung gestellt werden
- IT-Kontrollsystem
- wesentlicher Bestandteil des Internen Kontrollsystems

SerNet

Aufbau- / Funktionsprüfung

- IT-Strategie
- IT-Umfeld
- IT-Organisation
- Sicherheitsanforderungen
  - Vertraulichkeit, Verfügbarkeit, Integrität
  - Authorisierung, Authentizität, Verbindlichkeit

SerNet

IT-Infrastruktur

- Physische Sicherungsmaßnahmen
- Logische Zugriffskontrollen
- Datensicherungs- und Auslagerungsverfahren
- Maßnahmen für Regelbetrieb
- Maßnahmen für Notbetrieb
- Sicherung der Betriebsbereitschaft (Monitoring / Wartung)

SerNet

IT-Anwendungen

- Entwicklung von Individualsoftware
- Entwicklungsprozess und Pflege der IT-Anwendungen
- Auswahl und Beschaffung von Standardsoftware
- Test-und Freigabeverfahren für IT-Anwendung
- Änderung von IT-Anwendungen
- Verfahrensdokumentation und Archivierung
- Angemessenheit der rechnungslegungsrelevanten Verarbeitungsregeln
- Funktionsfähigkeit und Wirksamkeit der Programmfunktionen

SerNet

IT-gestützte Geschäftsprozesse

- Daten- und Belegfluss
- Kontroll- und Abstimmverfahren

SerNet

IT-Überwachungssystem

- High-Level-Controls
- Interne Revision
- Externe Revision

SerNet

IT-Outsourcing

- Eigentumsrechte / Verfügbarkeit von Software
- Datensicherung
- Freigabeverfahren
- Verantwortung bei fehlerhafter Bearbeitung
- Verfügungsrecht / Zugriff auf Dokumentation
- Sicherstellung der Vertraulichkeit
- Einsichtsrechte

SerNet

Internetnutzung

- Webseite, E-Mail, WWW
- EDI, E-Business
- Übergänge von Unternehmensnetzwerk in fremde bzw. unsichere Netzwerke (Firewall, Virenscanner...)
- Protokollierungs- und Überwachungsanforderungen zur rechtzeitigen Erkennung sicherheitsrelevanter Ereignisse
- Änderungen der IT-Infrastruktur oder sicherheitsrelevanter IT-Komponenten (Change Management)
- Herstellung geforderter Verfügbarkeit der Internet-Systeme

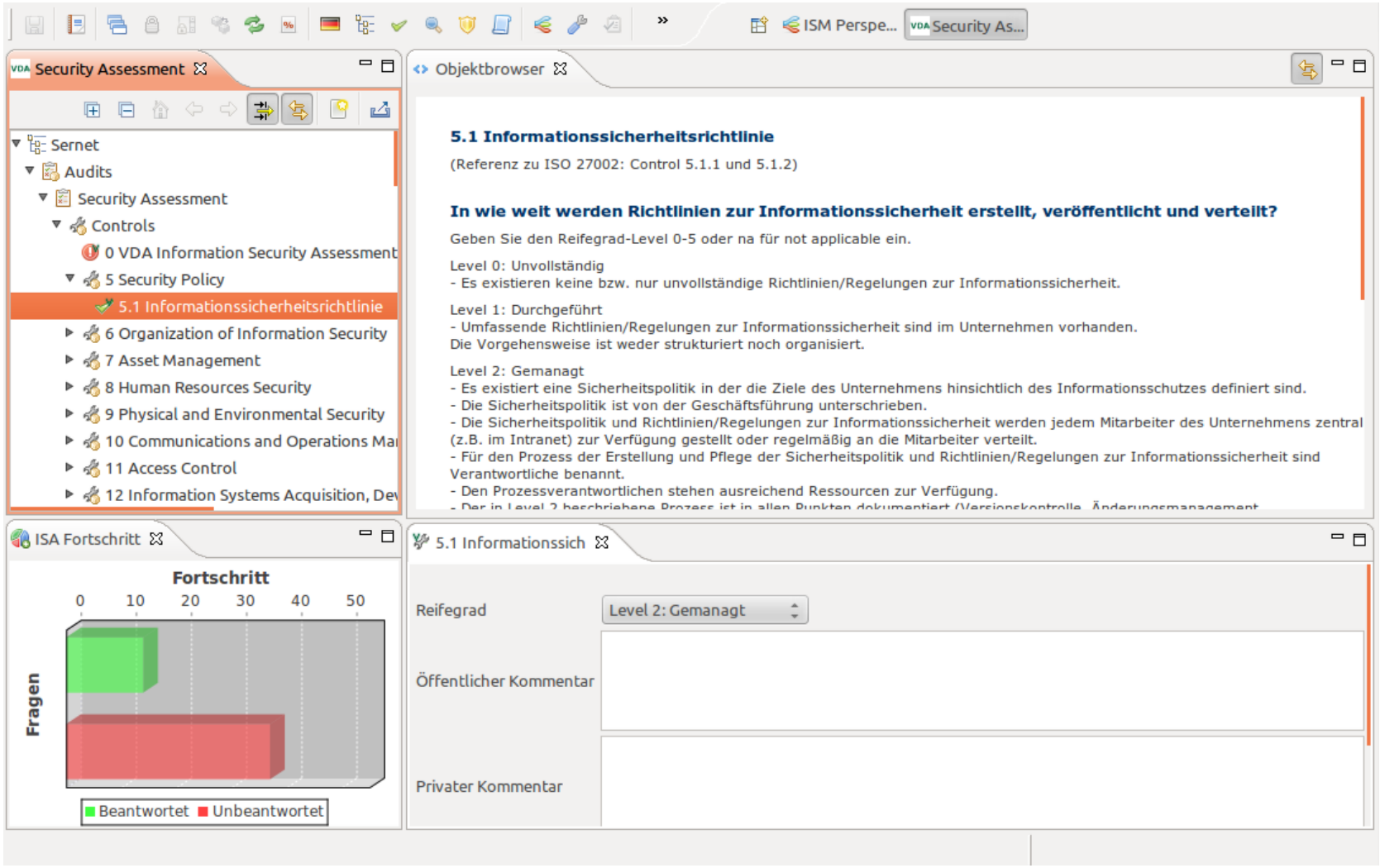
SerNet

IDW PS 330: Outsourcing

- Outsourcing ist z.B.
  - Übertragung von Rechenzentrums-Dienstleistungen
  - Provider bei Prozessen, die das Internet nutzen
  - Administration / Wartung von Standardsoftware durch externe Dienstleister
- Verantwortung verbleibt bei gesetzlichen Vertretern
- fordert vorhandes SiKo / Einsichtsrechte
  - => so werden Anforderungen weitergereicht

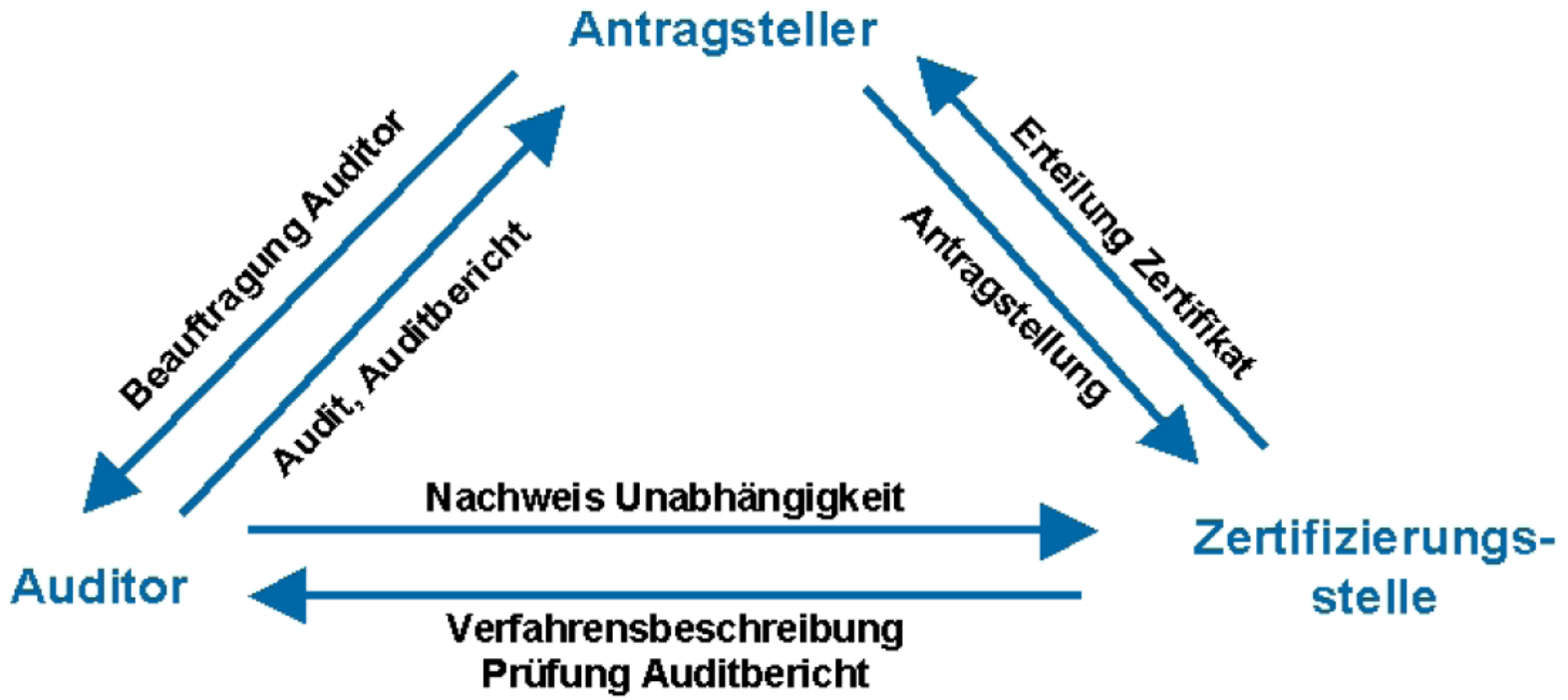
VDA ISA

SerNet



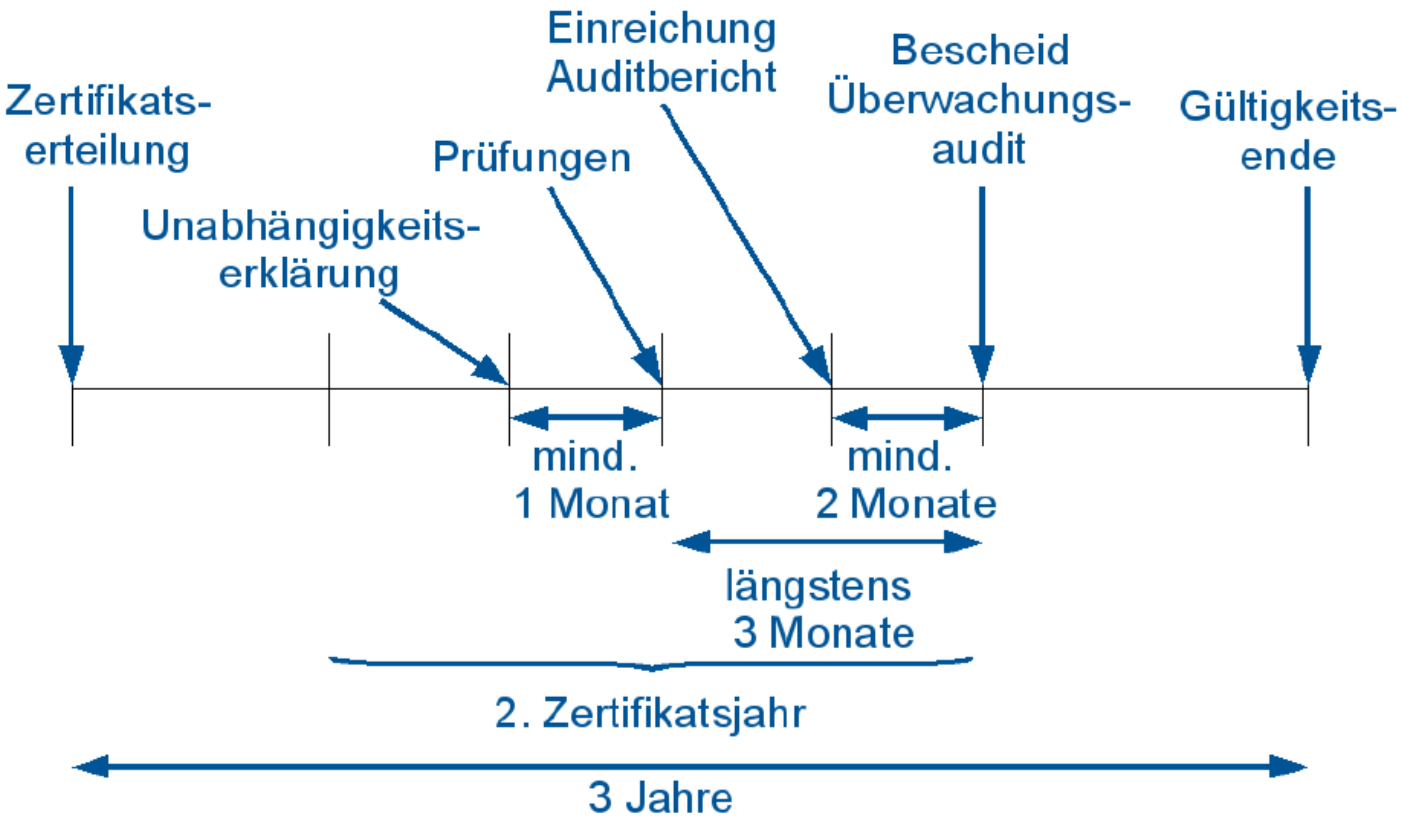
ISO 27001 / IT-Grundschutz

SerNet



ISO 27001 / IT-Grundschutz

SerNet



Übersicht

SerNet

- Wieso werde ich auditiert?
  - IS-Audits, Grundlagen, Standards
- Was erwartet mich?
  - Inhalte, Prüftiefe, Vorgehensweisen
- Was muss ich tun?
  - Vorbereitung, Begleitung, Reaktion

Vorbereitung

SerNet

- gute IT (-Governance) haben
- Projektpate in der GF
- IS-Beauftragter
- Datenschutzbeauftragter
- IS-Team

Vorbereitung

SerNet

- IS-Richtlinien
- IS-Aufzeichnungen
- Verträge / -vorlagen
- Schulung / Sensibilisierung

Das Audit

SerNet

- Auditplan
  - Termine, Ansprechpartner
- Vor-Audit
  - Dokumentenprüfung, Scans, Informationsbeschaffung
- Vor-Ort-Audit
  - Begehung, Befragungen, Inaugenscheinnahme...
- Auditbericht
  - Abweichungen, Empfehlungen

Kontakt

SerNet

Alexander Koderman, AK@sernet.de

SerNet GmbH

Bahnhofsallee 1b
37081 Göttingen

Schützenstr. 18
10117 Berlin

tel +49 551 370000-0
fax +49 551 370000-9

+49 30 5 779 779 0
+49 30 5 779 779 9

http://www.sernet.de