it.sec
security for your information

Praxiserfahrungen über die Aussagekraft von 27001-Zertifikaten

Holger Heimann
CEO it.sec
ISO/IEC 27001 Lead Auditor, CISA, CRISC, gepr. Datenschutzbeauftrager

Workshop GI-FG SECMGT – „Wert von Zertifizierungen“
Frankfurt am Main, 7.6.2013

About it.sec

- Specialized in Information Security and Privacy, delivering
  - Classical Information Security Consulting
  - IT Governance- Risk- & Compliance Consulting
  - Penetration Testing
  - IT-Forensics, eDiscovery & internal investigations
- Founded in 1996
- Servicing e.g. Banking and Finance, Pharmaceutics, Automotive & Industrial Production, GOs, NGOs etc.

About Holger Heimann

- Senior Information Security Consultant
- > 25 Years in IT
- Dipl-Ing(FH), CEO it.sec, CISA, CRISC, Certified Privacy Protection Professional, Cert. ISO/IEC 27001 Lead Auditor
- Contributor to tools like nmap, nikto and nessus
- Author of many magazin articles
- Former University Lecturer
- Etc.

Warum überhaupt Zertifizierungen nach ISO/IEC 27001?

Harte Argumente:

- Entlastung des Managements durch Erfüllung der Sorgfaltspflicht
- Reduktion von Haftungsrisiken, ggf. Beweislastumkehr
- Ggf. Vorteile bei Versicherungen
- Zwang durch Auftraggeber

Innenwirkung:

- Überprüfung der eigenen Sicherheitsstandard gegen „Best Practises“
- Vorsorge durch Identifizieren, Bewerten und Beherrschen von IS-Risiken
- Dokumentation von Strukturen und Prozesse

Aussenwirkung:

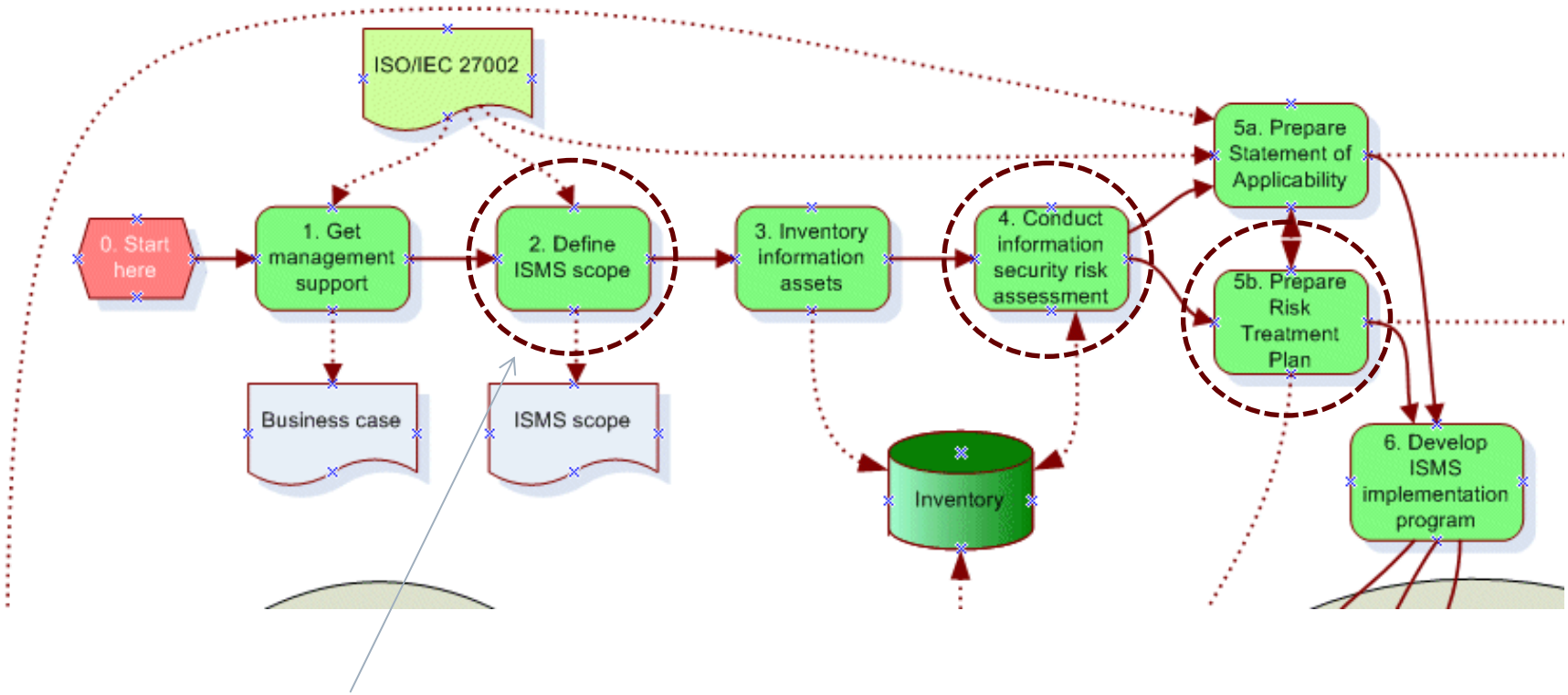
- Nachweis der Sicherheit/Compliance gegenüber Dritten (Kunden, Partner, WP, Gesetzgeber …)
- Pot. Auditentlastung für alle Beteiligten
- Wettbewerbsvorteil („dokumentierte Qualität“)
- Reduzierung der Marktzutrittsbarrieren für den nationalen und internationalen Markt
- bessere Kundenbindung und –neugewinnung
  - Sehr viele IT-Dienstleister zertifiziert!

ISO/IEC 27001 im Auftraggeber-Auftragnehmer Verhältnis

Was wird eigentlich zertifiziert?

- ISO/IEC 27001 zertifiziert ein ISMS, ein „Informationssicherheits-Managementsystem“
- Zertifiziert wird also der definierte *Umgang* mit Informationssicherheits-Anforderungen im Rahmen von Best-Practises
  - nicht der Grad der erreichten Sicherheit

Vorgehen ISO/IEC 27001

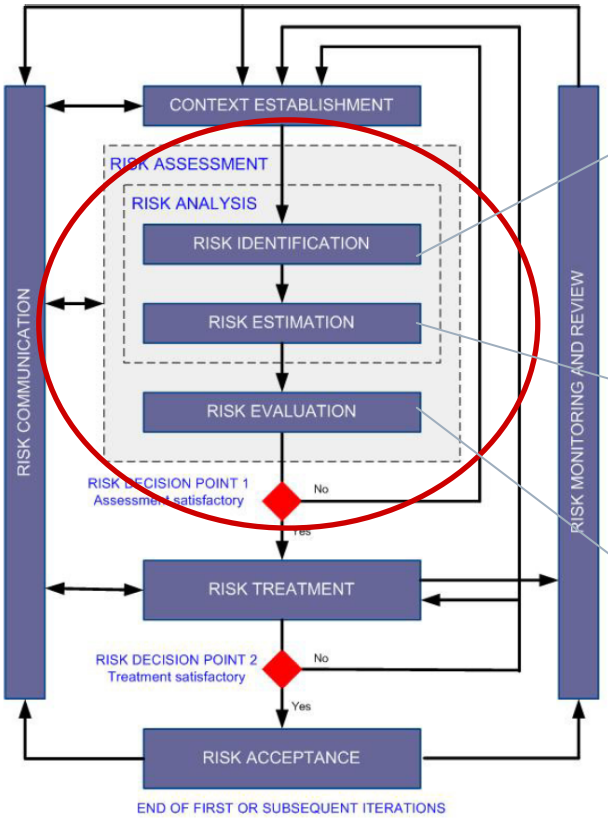


Scope

- Der Anwendungsbereich des ISMS erstreckt sich oft nur über Teilbereiche der IT Landschaft oder bestimmte Locations
  - „Datenannahme“
  - „Web-Hosting“
  - „Standort München“
- Legt auch die Anforderungen fest
  - Business-, rechtliche- und vertragliche Anforderungen …
- Beim Outsourcing vom Management von IT Services eher selten auf die Kundenbereiche

Risk Assessment

- IT-Risikomanagementprozess nach der ISO/IEC 27005



- Bedeutung:

Risk Assessment besteht aus:

- <u>Risikoidentifikation</u>
  - ° Bestimmung relevanter Assets (Prozesse, IT-Systeme, Personen, Daten)
  - ° Bestimmung der Bedrohungen
  - ° Bestimmung der Verwundbarkeiten
- <u>Risikoanalyse</u>
  - ° Ermittlung Eintrittswahrscheinlichkeiten
  - ° Ermittlung potenzieller Schadensauswirkungen
- <u>Risikobewertung</u>
  - ° Priorisierung von zu adressierenden Risiken

Was ist “Risiko”?

Eintrittswahrscheinlichkeit x Schadenshöhe

… oder ist es…

Verletzlichkeiten x Eintrittswahrscheinlichkeit x Schadenshöhe /Gegenmaßnahmen

… oder noch was anderes …?

Wie wird bewertet?

- Quantitativ?
- Qualitativ?
  - „Nieder, Mittel, Hoch?“

- Bezugnehmend auf welche Schutzziele?
  - Vertraulichkeit – Verfügbarkeit – Integrität
  - Oder auch Authentizität, Verbindlichkeit?
  - Oder „Eintritt eines Fehlerfalls“
  - …

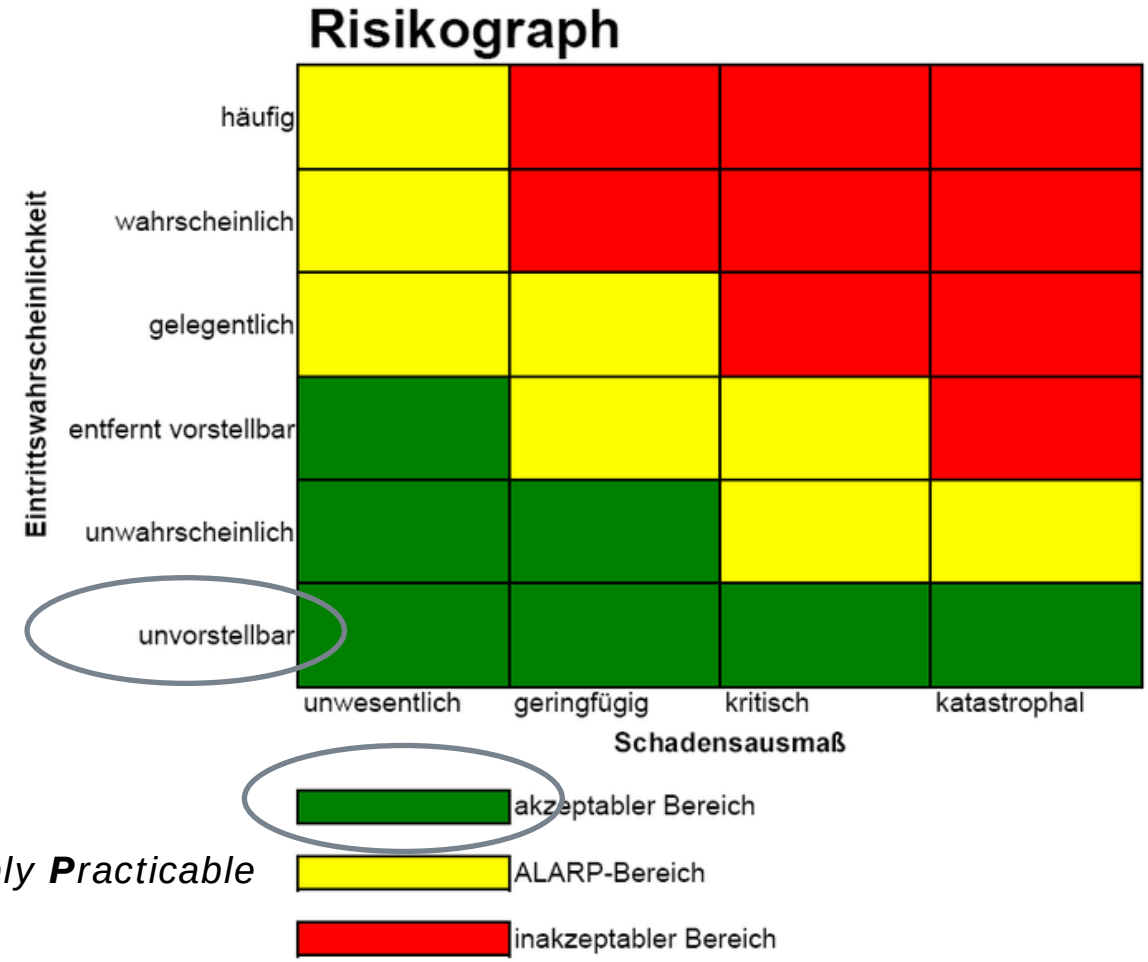
4.2.1 c) 1) Identify a risk assessment methodology

ISO/IEC 31010 RA Methodologies

Tools and techniques	Risk assessment process					See Annex
	Risk Identification	Risk analysis			Risk evaluation	
		Consequence	Probability	Level of risk		
Brainstorming	SA[1)]	NA[2)]	NA	NA	NA	B 01
Structured or semi-structured interviews	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Check-lists	SA	NA	NA	NA	NA	B 04
Primary hazard analysis	SA	NA	NA	NA	NA	B 05
Hazard and operability studies (HAZOP)	SA	SA	A[3)]	A	A	B 06
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA	B 07
Environmental risk assessment	SA	SA	SA	SA	SA	B 08
Structure « What if? » (SWIFT)	SA	SA	SA	SA	SA	B 09
Scenario analysis	SA	SA	A	A	A	B 10
Business impact analysis	A	SA	A	A	A	B 11
Root cause analysis	NA	SA	SA	SA	SA	B 12
Failure mode effect analysis	SA	SA	SA	SA	SA	B 13
Fault tree analysis	A	NA	SA	A	A	B 14
Event tree analysis	A	SA	A	A	NA	B 15

Restrisikoakzeptanz

Beispiel:
Typische,
qualitative
Risikomatrix



***A**s **L**ow **A**s **R**easonably **P**racticable*

Quelle: Wikipedia

Umgang mit Risiken – Risk Treatment

- Risiken kann man (z.B:)
  - Vermeiden (Avoid)
  - Mindern (Mitigate)
  - Übertragen (Transfer)
  - Akzeptieren (Accept)

- Potentiell unterschiedliche Sicht bei den Partnern – i.d.R. nicht transparent.
- → „Hunderte lokale Admins“

Subjektivität der Impact/Risikoeinschätzung

- Wer hat schon Umfragen zu Verfügbarkeits-anforderungen im Unternehmen gemacht?
- Wie hoch ist die Wahrscheinlichkeit von irgendwas, wenn keine statistische Basis vorliegt?
- Psycho- & Physiologie
  - Sprache und Situationsbewertung (Einsatz € 1, Gewinn 1.50)
  - Entscheidungen und der Blutzuckerspiegel (1€ heute oder 2 morgen)

Risikoeinschätzung sind (gemäß Anforderung) reproduzierbar

nicht aber unbedingt vergleichbar

Unterschiedliche Sicht auf Risiken

- Der Outsourcer sieht andere Risiken als der Auftraggeber
  - (Security) Incident Management als Risiko?
  - Akzeptanz von Risiken ggf. anders
  - Schadenshöhen teils per gedeckelter Pönale (im Gegensatz zum Auftraggeber)

- Anforderungen den Kunden i.d.R. als SLA definiert, beim Reißen Strafzahlungen
  - Risikomanagement des Outsourcers?

Vorgaben des Auftraggebers

- 27001 4.2.1 Establish the ISMS

  b) 2): Define a ISMS Policy that … takes into account business and legal or regulatory requirements, **and contractual security obligations**

- Realitycheck: oft werden dem Auftraggeber schon Vorlagen mitgeliefert

A.13.2 Management of information security incidents and improvements

A.13.2.3	Collection of evidence	*Control* Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

- Weiß der Outsourcingpartner wann „legal action“ angezeigt ist?
- Haben die Parteien die gleiche Sicht auf Security Incidents und deren Nachvollziehbarkeit?
  - Legal vg. SLA Risiko
  - Bsp. Rechtevergabe, Beispiel Malware

Audit Rechte

- Oft nur als Papierkontrollen durchführbar („Shared Service Provider“)
- Keine generelle Offenlegungspflicht hinsichtlich
  - der identifizierten Risiken
  - der genauen Risikobehandlung
  - der Restrisikoakzeptanz
- Nur die getroffenen Maßnahmen sind i.d.R. einsehbar (über Controls)

Worauf also achten?

- Bei zertifizierten Anbietern Scope prüfen!
- Eigene Sicherheitsvorgaben vertraglich festlegen!
  - Insbesondere Augenmerk auf (Security!) Incident Management legen!
- Ist das Outsourcingmodell passend oder gibt es Schwierigkeiten z.B. bei Beweissicherungen?
- Meine Risiken sind nicht Deine Risiken
- Outsourcing als eigenes Risiko betrachten!
- Pönalen in Relation zum eigenen Risiko sehen.
- „You get what you pay for“

Any Questions?

Siehe auch:

SecuMedia Verlag

<kes> Nr. 2, März 2013

Seite 6: „*Der schöne Schein*“

Danke für Ihre Aufmerksamkeit!

Quellen

- Fremde Sprache, bessere Entscheidungen: http://www.karriere.de/karriere/fremde-sprache-bessere-entscheidungen-164845
- Kognitive Verzerrungen: http://de.wikipedia.org/wiki/Prospect_Theory
- Entscheidungen und Blutzuckerspiegel: http://www.welt.de/wissenschaft/article5989639/Eine-Entscheidung-haengt-auch-vom-Blutzucker-ab.html

it.sec GmbH & Co. KG
Sedanstraße 10
D-89077 Ulm

USt Id Nr.: DE 225547544
Steuernummer: 88012/53709
Amtsgericht Ulm: HRA 3129

vertreten durch den **Geschäftsführer Dipl. Ing. (FH) Holger Heimann**.

Haftender Komplementär:
it.sec Verwaltungs GmbH
Amtsgericht Ulm: HRB 4593
Einsteinstr. 55
D-89077 Ulm

tel: +49 (0) 731 20589-0
mailto:info@it-sec.de
http://www.it-sec.de