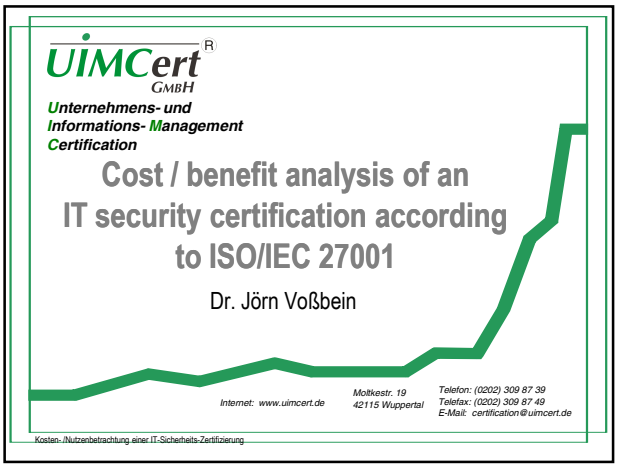
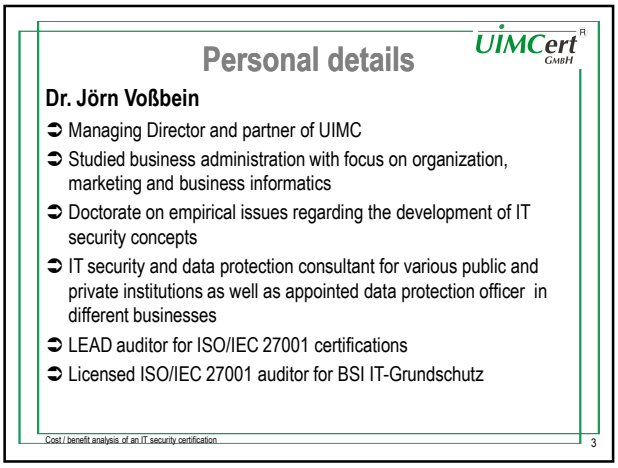
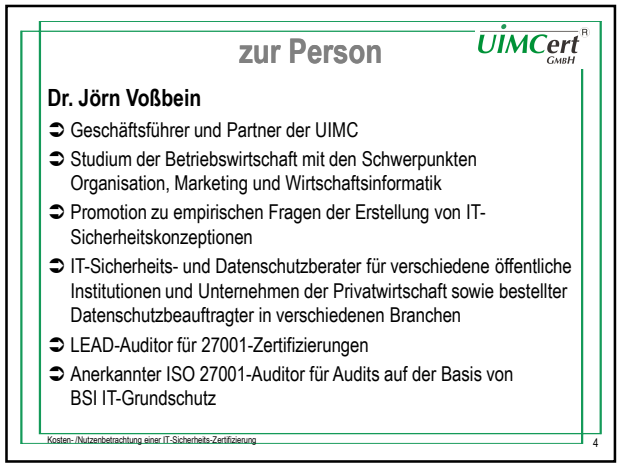
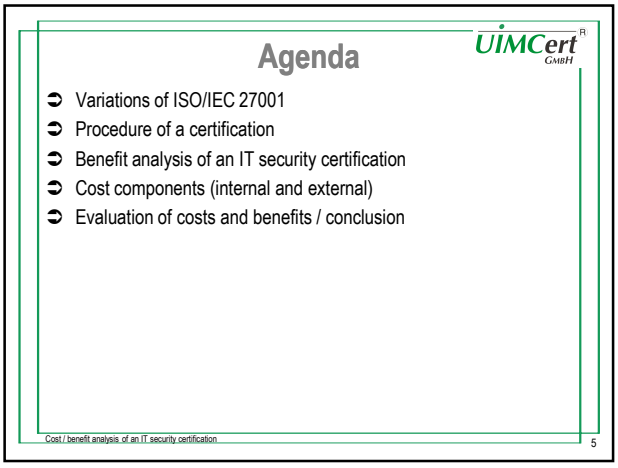
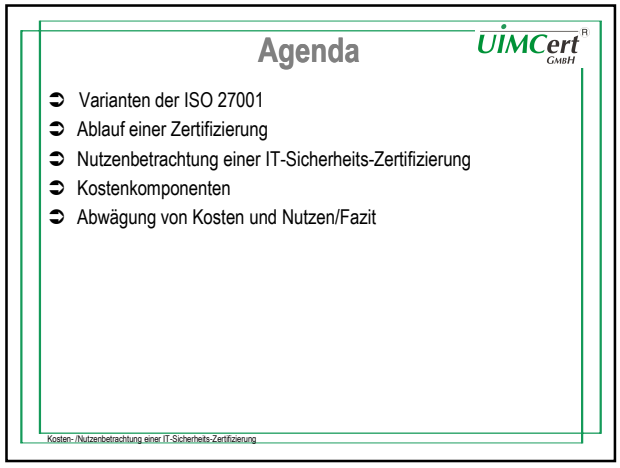

UIMCert GmbH
Unternehmens- und
Informations- Management
Certification
Cost / benefit analysis of an
IT security certification according
to ISO/IEC 27001
Dr. Jörn Voßbein
Internet: www.uimcert.de
Moltkestr. 19
42115 Wuppertal
Telefon: (0202) 309 87 39
Telefax: (0202) 309 87 49
E-Mail: certification@uimcert.de
Kosten- /Nutzenbetrachtung einer IT-Sicherheits-Zertifizierung


UIMCert GmbH
Unternehmens- und
Informations- Management
Certification
Kosten- / Nutzenbetrachtung einer
IT-Sicherheits-Zertifizierung nach
ISO 27001
Dr. Jörn Voßbein
Internet: www.uimcert.de
Moltkestr. 19
42115 Wuppertal
Telefon: (0202) 309 87 39
Telefax: (0202) 309 87 49
E-Mail: certification@uimcert.de
Kosten- /Nutzenbetrachtung einer IT-Sicherheits-Zertifizierung

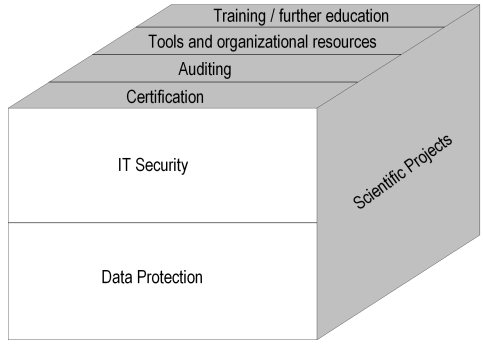

Personal details
UIMCert GmbH
Dr. Jörn Voßbein
Managing Director and partner of UIMC
Studied business administration with focus on organization, marketing and business informatics
Doctorate on empirical issues regarding the development of IT security concepts
IT security and data protection consultant for various public and private institutions as well as appointed data protection officer in different businesses
LEAD auditor for ISO/IEC 27001 certifications
Licensed ISO/IEC 27001 auditor for BSI IT-Grundschutz
Cost / benefit analysis of an IT security certification
3


zur Person
UIMCert GmbH
Dr. Jörn Voßbein
Geschäftsführer und Partner der UIMC
Studium der Betriebswirtschaft mit den Schwerpunkten Organisation, Marketing und Wirtschaftsinformatik
Promotion zu empirischen Fragen der Erstellung von IT-Sicherheitskonzeptionen
IT-Sicherheits- und Datenschutzberater für verschiedene öffentliche Institutionen und Unternehmen der Privatwirtschaft sowie bestellter Datenschutzbeauftragter in verschiedenen Branchen
LEAD-Auditor für 27001-Zertifizierungen
Anerkannter ISO 27001-Auditor für Audits auf der Basis von BSI IT-Grundschutz
Kosten- /Nutzenbetrachtung einer IT-Sicherheits-Zertifizierung
4


Agenda
UIMCert GmbH
Variations of ISO/IEC 27001
Procedure of a certification
Benefit analysis of an IT security certification
Cost components (internal and external)
Evaluation of costs and benefits / conclusion
Cost / benefit analysis of an IT security certification
5

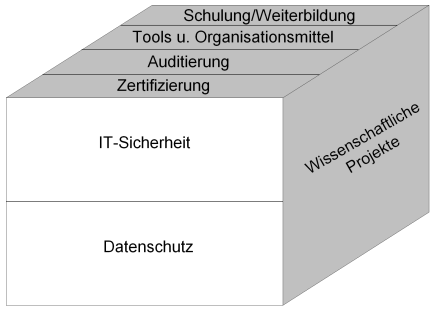

Agenda
UIMCert GmbH
Varianten der ISO 27001
Ablauf einer Zertifizierung
Nutzenbetrachtung einer IT-Sicherheits-Zertifizierung
Kostenkomponenten
Abwägung von Kosten und Nutzen/Fazit
Kosten- /Nutzenbetrachtung einer IT-Sicherheits-Zertifizierung

UIMCert´s sphere of action



Cost / benefit analysis of an IT security certification 7

Tätigkeitsfeld der UIMCert



Kosten- /Nutzenbetrachtung einer IT-Sicherheits-Zertifizierung

Variations of ISO/IEC 27001

native

- Internationally acknowledged
- Based on the general structure of standards
- **Risk orientation** (incl. probability)
- PDCA for the whole management system
- Orientation towards **critical** business processes

based on BSI IT-Grundschutz

- Nationally oriented and acknowledged
- Highly different from general ISO/IEC standards
- Simple consideration of risks
- PDCA only for the IT security concept
- Basis: GS-Katalog and layer model

Cost / benefit analysis of an IT security certification 9

Varianten der ISO 27001

native

- international geprägt und anerkannt
- Orientierung am allgemeinen Normenaufbau
- **Risiko-Orientierung** (inkl. Wahrscheinlichkeit)
- PDCA für gesamtes Managementsystem
- Orientierung an **kritischen** Geschäftsprozessen

auf Basis BSI IT-Grundschutz

- nationale Prägung und Anerkennung
- stark von allgemeinen ISO-Normen abweichend
- einfache Betrachtung der Gefährdungen
- PDCA nur für das IT-Sicherheitskonzept
- Basis: GS-Kataloge und Schichtenmodell

Kosten- /Nutzenbetrachtung einer IT-Sicherheits-Zertifizierung

Certification and auditing

Certification according to ISO/IEC 27001

- Predominance of the management components (not the technical aspects)
- Great importance of security policy:
  - » without consistent, explicitly formulated and communicated security policy, no ISMS can be permanently successful
- Auditing and certification of subsystems, e.g.
  - » Computing centres, Business Continuity System…
- Limited validity: usually 3 years

Cost / benefit analysis of an IT security certification 11

Zertifizierung und Auditierung

Zertifizierung nach ISO/IEC 27001

- Dominanz der Managementkomponenten (nicht der technischen Aspekte)
- hohe Bedeutung der Sicherheitspolitik:
  - » ohne konsistente, explizit formulierte und kommunizierte Si-Politik kann kein ISMS auf Dauer erfolgreich sein
- Auditierung und Zertifizierung von Teilsystemen möglich, z. B.
  - » Rechenzentren, Notfallmanagementsystem...
- beschränkte Gültigkeitsdauer: i. d. R. 3 Jahre

Kosten- /Nutzenbetrachtung einer IT-Sicherheits-Zertifizierung

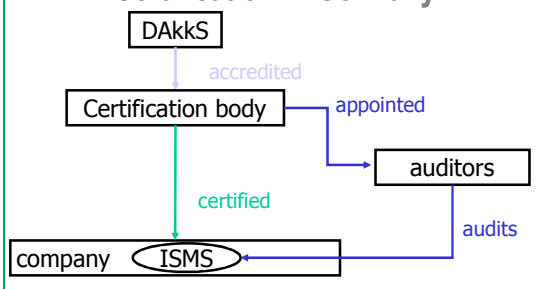
Procedure of a certification process

- Setting audit dates and creating audit plans
- Documentation evaluation
- On-site audit (random review of the implemented management system)
- Creating the audit reports and defining corrective measures
- Post audit after elimination of deviations – if necessary
- Certificate issuance with registration

Ablauf eines Zertifizierungsverfahrens

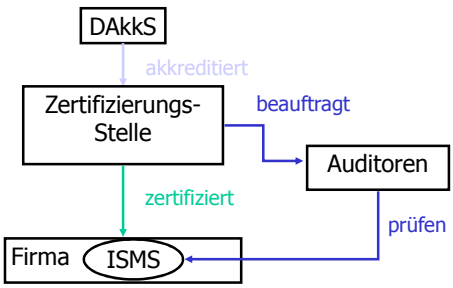
- Audittermine festlegen und Auditplan erstellen
- Dokumentationsprüfung
- Vor-Ort-Prüfung (Stichprobenartige Überprüfung des implementierten Managementsystems)
- Auditbericht erstellen und Korrekturmaßnahmen festlegen
- Nachaudit nach Beseitigung von Abweichungen – falls erforderlich
- Zertifikatserstellung mit Registrierung

Certification in Germany



Different (more complex) process for ISO/IEC 27001 based on BSI IT-Grundschutz

Zertifizierung in Deutschland



Abweichendes (komplexeres) Verfahren bei ISO 27001 auf Basis BSI IT-Grundschutz

Certification cycle

- Initial audit – first certification
  The certificate is usually valid for 3 years
- Monitoring audit/periodical audits (annual)
  The certificate´s validity is extended by semiannual or annual service visits. Subsections of clients are also audited.
- Re-audit – recertification
  After 3 years follows a renewal of the certificate. The entire system will be checked again.

Zertifizierungsabfolge

- Initialaudit – Erstzertifizierung
  Das Zertifikat hat in der Regel eine Laufzeit von 3 Jahren
- Überwachungsaudit/Periodische Audits (jährlich)
  Durch halbjährliche bzw. jährliche Betreuungsbesuche wird das Zertifikat aufrechterhalten. Hierbei werden Teilbereiche des Kunden auditiert.
- Wiederholungsaudit – Rezertifizierung
  Nach 3 Jahren erfolgt die Zertifikatserneuerung. Hierbei wird das gesamte System erneut geprüft.

Alternative opportunities

- UIMCert attestation IT security
- UIMCert attestation privacy protection

- Certificate ISO/IEC 27001
- Certificate ISO/IEC 27001 based on BSI IT-Grundschutz
- Certificate ISO/IEC 27001 certification of the privacy protection subsystem

Alternative Möglichkeiten

- UIMCert Testat IT-Sicherheit
- UIMCert Testat Datenschutz

- Zertifikat ISO/IEC 27001
- Zertifikat ISO/IEC 27001 auf Basis BSI IT-Grundschutz
- Zertifikat ISO/IEC 27001 Zertifizierung des Datenschutz Subsystems

Internal benefits of the certification

Internal effects (partially by the previous auditing)

- Intensive preoccupation with the IT security system by employees and third parties
- Increase of IT security of the entire system or major parts
- Opportunity to focus on especially sensitive security parts of the system
- Increase of image value among employees and third parties regarding IT security
- Cost-steering effects in terms of operational cost optimization
- Protection against „suspicions of organizational faults“

Interner Nutzen der Zertifizierung

Innenwirkung (teilweise durch die vorausgehende Auditierung)

- Intensive Beschäftigung mit dem IT-Sicherheitssystem durch eigene Mitarbeiter und Dritte
- Erhöhung der IT-Sicherheit des Gesamtsystems oder wesentlicher Teile
- Möglichkeit, sich auf besonders sicherheitssensitive Teile des Gesamtsystems zu konzentrieren
- Erhöhung des Imagewertes in Sachen IT-Sicherheit bei Mitarbeitern und Dritte
- Kostenlenkungseffekte im Sinne von Kosteneinsatzoptimierung
- Schutz gegen „Verdacht des Organisationsverschulden“

External benefits of the certification

External effects

- Preservation of a publicity effective certificate on security quality
- Increase of image value among external reference groups regarding IT security
- Revenue and profit growth by increasing confidence at sales relevant reference groups
- Security as a quality criterion
- Assignment of dealing with IT security issues (KonTraG)

Externer Nutzen der Zertifizierung

Außenwirkung

- Erhalt eines publicity-wirksamen Zeugnisses über die Sicherheitsqualität
- Erhöhung des Imagewertes in Sachen IT-Sicherheit bei externen Bezugsgruppen
- Erlös- und Gewinnzuwächse durch Vertrauenserhöhung bei umsatzrelevanten Bezugsgruppen
- Sicherheit als Qualitätskriterium
- Belegung der Auseinandersetzung mit der IT-Sicherheitsproblematik (KonTraG)

Costs/expense of a 27001 certificate (I)

Based on ISO 27006

- Additional expense for several locations (multiple sites)
- Thereof monitoring audit approx.1/3, reaudit approx. 2/3
- Influencing factors:

Increasing expense factors:	Decreasing expense factors:
» several locations	» no/low risk product/processes
» high degree of regulation	» knowledge of the organization
» complex ISMS processes	» preparedness for certification
	» mature management system

Cost / benefit analysis of an IT security certification 25

Kosten/Aufwand eines 27001-Zertifikats

auf Basis ISO 27006

- Mehraufwand bei mehreren Standorten
- davon Überwachungsaudit ca. 1/3, Reaudit ca. 2/3
- Beeinflussende Faktoren…

Aufwandserhöhend:	Aufwandsmindernd:
» mehrere Standorte	» keine/wenige Risikoverfahren
» mehrsprachige Angestellte	» Fachwissen d. Unternehmens
» komplexe ISMS-Verfahren	» Zertifizierungsvorbereitung
	» reifes Managementsystem

Kosten- /Nutzenbetrachtung einer IT-Sicherheits-Zertifizierung

Cost/expense of a 27001 certificate (II)

Auditor Time Chart (extract 27006 Annex C)

Number of Employees	ISMS Auditor Time for Initial Audit (auditor days)
1 ~ 10	5
46 ~ 65	10
126 ~ 175	13
626 ~ 875	17,5
2026 ~ 2675	22
4351 ~ 5450	25
8501 ~ 10700	28

Cost / benefit analysis of an IT security certification 27

Kosten/Aufwand eines 27001-Zertifikats

Auditorzeitdiagramm (Auszug 27006 Annex C)

Anzahl der Angestellten	ISMS Auditorzeit für Initialaudit (Auditortage)
1 ~ 10	5
46 ~ 65	10
126 ~ 175	13
626 ~ 875	17,5
2026 ~ 2675	22
4351 ~ 5450	25
8501 ~ 10700	28

Kosten- /Nutzenbetrachtung einer IT-Sicherheits-Zertifizierung

Cost of a BSI certificate

- For each certification process, the BSI generally charges 2.500 Euro
- Cost of the auditing are usually clearly higher than a native certification
  - Audit procedure
  - Audit depth
  - Feedback by BSI

Cost / benefit analysis of an IT security certification 29

Kosten eines BSI Zertifikats

- für jedes Zertifizierungsverfahren erhebt das BSI pauschal 2.500 Euro
- Kosten der Auditierung i. d. R. deutlich höher als bei einer nativen Zertifizierung
  - Prüfverfahren
  - Prüftiefe
  - Rückkoppelungen mit BSI

Kosten- /Nutzenbetrachtung einer IT-Sicherheits-Zertifizierung

Evaluation of costs and benefits / conclusion

- High benefits from occupation with the ISMS and an improved IT security system
- Internal costs are not attributable and a multiplicity of the external costs
- Benefit normally not quantifiable
  - » possible K.O.-criterion for assignments
- Certificate´s value is highly dependent on the businesses

Abwägung von Kosten und Nutzen/ Fazit

- Interne Kosten schlecht zurechenbar und ein Vielfaches der Externen
- Hoher Nutzen durch Auseinandersetzung mit dem ISMS sowie ein verbessertes IT-Sicherheitssystem
- Nutzen i.d.R. nicht berechenbar
  - » ggf. K.O.-Kriterium bei Aufträgen
- Wertigkeit der Zertifikate stark branchenabhängig

Questions??

UIMC DR. VOSSBEIN GMBH & CO. KG
Nützenberger Straße 119
42115 Wuppertal
Telefon: (0202) 265 74 - 0
Telefax: (0202) 265 74 - 19
E-Mail: consultants@uimc.de
URL: www.UIMC.de

UIMCert GmbH
Moltkestraße 19
42115 Wuppertal
Telefon: (0202) 3 09 87 39
Telefax: (0202) 3 09 87 49
E-Mail: certification@uimcert.de
URL: www.UIMCert.de

Fragen??

UIMC DR. VOSSBEIN GMBH & CO. KG
Nützenberger Straße 119
42115 Wuppertal
Telefon: (0202) 265 74 - 0
Telefax: (0202) 265 74 - 19
E-Mail: consultants@uimc.de
URL: www.UIMC.de

UIMCert GmbH
Moltkestraße 19
42115 Wuppertal
Telefon: (0202) 3 09 87 39
Telefax: (0202) 3 09 87 49
E-Mail: certification@uimcert.de
URL: www.UIMCert.de