UIMCert GmbH
Unternehmens- und Informations- Management Certification

Risikomanagement und IT-Sicherheit in der 8. EU-Richtlinie und ihre Prüfung

Dr. J. Voßbein

Internet: www.uimcert.de

Moltkestr. 19
42115 Wuppertal

Telefon: (0202) 309 87 39
Telefax: (0202) 309 87 49
E-Mail: certification@uimcert.de

Begrüßung - Vorstellung des Referenten

UIMCert

Dr. Jörn Voßbein,

Geschäftsführer und Partner der UIMC Dr. Voßbein GmbH & Co KG

- **Studium der Betriebswirtschaft mit den Schwerpunkten Organisation, Marketing, Wirtschaftsinformatik an der Universität zu Köln mit Abschluss Diplom-Kaufmann**
- **Promotion zu empirischen Fragen der Erstellung von IT-Sicherheitskonzeptionen**
- **Extern bestellter Datenschutzbeauftragter in zahlreichen Institutionen verschiedener Branchen**
- **IT-Sicherheits- und Datenschutzberatung für verschiedene öffentliche Institutionen und Unternehmen der Privatwirtschaft**
- **Leiter GDD-Erfa-Kreis Bergisches Land**
- **BSI lizenzierter Auditor für ISO/IEC 27001 auf Basis IT-Grundschutz**

jvossbein@uimc.de

UIMCert

Ziel der folgenden Ausführungen ist nicht:

- **Überblick über die 8. EU-Richtlinie zu geben**
- **Konsequenzen für die Gesetzgebung in Deutschland aufzuzeigen**

Ziel der folgenden Ausführungen ist:

- **Konsequenzen der 8. EU-Richtlinie für die praktische Prüfarbeit aufzuzeigen**
- **Hilfen für die Prüfarbeit zu geben**

UIMCert

Inhalt

Auszug aus der Richtlinie

Besondere Bestimmungen für Unternehmen im „öffentlichen Interesse“

- Einrichtung eines Prüfungsausschusses (audit comittee)
- Mitglieder müssen Verwaltung oder Aufsichtsrat angehören
- dürfen nicht zur Geschäftsleitung gehören
- min. ein Mitglied unabhängig und kompetent im Bereich Rechnungslegung und / oder Abschlussprüfung

Ziel: ***Verhinderung einer Einflussnahme der Geschäftsführung auf die Abschlussprüfung.***

Überwachung des Rechnungslegungsprozesses von einer unternehmensinternen Instanz.

Die Aufgabe des Prüfungsausschusses besteht unter anderem darin, (...)

(b) **die Wirksamkeit der internen Kontrolle, gegebenenfalls der Innenrevision und des Risikomanagements des Unternehmens zu kontrollieren;**

Die im Rahmen der Eignungsprüfung durchgeführte theoretische Prüfung umfasst insbesondere die folgenden Sachgebiete:

(a) Theorie und Grundsätze des allgemeinen Rechnungswesens,

(b) gesetzliche Vorschriften und Grundsätze für die Aufstellung des Jahresbeschlusses und des konsolidierten Abschlusses,

(c) Internationale Rechnungsstandards,

(d) Finanzanalyse,

(e) Kosten- und Leistungsrechnung,

(f) Risikomanagement und interne Kontrolle.

UIMCert

Gesetzliche Grundlagen für ein Risikomanagement der IT-Sicherheit

IT-Sicherheitsbezogene ordnungsrechtliche Verhaltensverpflichtungen lassen sich unterteilen in:

- Vorsorgepflichten (z. B. Überwachung und Sicherung von Anlagen),
- Organisationspflichten (z. B. Bestellung eines Sicherheitsbeauftragten, Erarbeitung eines Sicherheitskonzepts, Dokumentationen) und
- überwachungserleichternde Pflichten (z. B. Auskunfts-, Mitteilungs-, sonstige Mitwirkungspflichten).

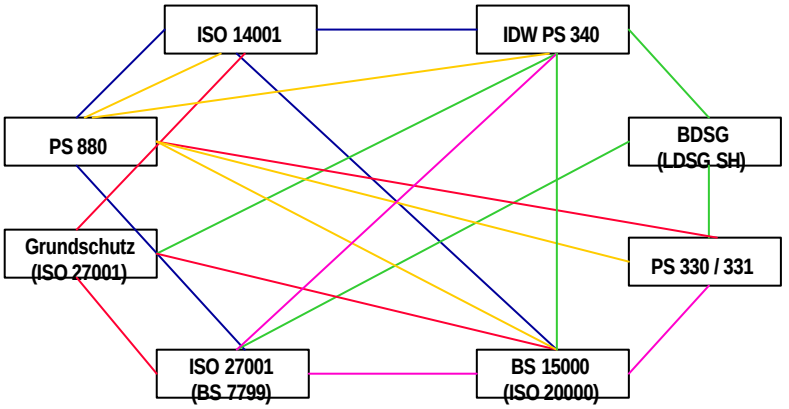
UIMCert

Zur Funktion von Standards und Normen in der IT

1. **Eine Norm**
   - ist eine Vorschrift zur vereinheitlichenden Gestaltung von Produkten, Prozessen oder Dienstleistungen.
   - geht davon aus, dass eine Realisierung gemäß ihren Anforderungen ausschließlich qualifiziertem und kompetentem Fachpersonal anvertraut wird.
   - setzt nicht voraus, dass ihre Befolgung gewährleistet, dass zum Beispiel Verträge oder gesetzliche Bestimmungen bei normenkonformer Gestaltung einwandfrei sind.
2. **Normenkonformität bedeutet daher ein dem Stand des Wissens und der Technik entsprechendes System.**
3. **In Bezug auf die Informationstechnologie und die IT-Sicherheit bedeutet daher die Anwendung und Befolgung der Forderungen einer Norm eine Konformität mit dem „State of the Art“ und damit eine relative Sicherheit, nicht an den Aktualisierungsanforderungen vorbei zu agieren.**

UIMCert

Vernetzung der Normen und Standards zum IT-Risiko-Management und zur IT-Sicherheit



UIMCert

Konkretisierung an Beispielen

Ordnungsmäßigkeitsprüfungen für folgende Beispiele:

- KonTraG
- Basel II
- IDW PS 340
- IDW PS 330
- IDW PS 880

Zielsetzungen des KonTraG:

- Unternehmensführungsmethoden zu installieren, die es möglich machen,
- Entwicklungen, die den Fortbestand des Unternehmens gefährden könnten, frühzeitig zu erkennen.

Als mögliche, die Existenz gefährdenden Entwicklungen werden insbesondere genannt:

- Risiko-behaftete Geschäfte
- Unrichtigkeiten
- Verstöße gegen gesetzliche Vorschriften

Betreffende Risiken haben Auswirkungen auf Vermögens-, Ertrags- und Finanzanlagen.

Basel II (EU-Eigenkapitalrichtlinie) (Capital Requirements Directive CRD)

- Ziel von Basel II ist es, die Stabilität im Kreditwesen zu erhöhen.
- Die Hinterlegung mit Eigenkapital bei den Kreditinstituten berücksichtigt die Risiken des einzelnen Kreditengagements.
- Die Höhe des zur Absicherung von Krediten einzusetzenden Eigenkapitals hängt wesentlich von der Bonität und den Zukunftsaussichten des Kreditnehmers ab.

Hierbei werden auch „weiche Faktoren“ in den kreditnehmenden Unternehmen überprüft und bewertet.

IDW PS 340

- **Der IDW Standard IDW PS 340 behandelt die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB.**
  Er behandelt die Maßnahmen, die nach dem KonTraG Gegenstand der Prüfung sind, wobei hierbei
  - die festgelegten Risikofelder
  - die Risikoerkennung und Risikoanalyse
  - die Risikokommunikation
  - die Zuordnung von Verantwortlichkeiten und Aufgaben
  - die Errichtung eines Überwachungssystem sowie
  - die Dokumentation der getroffenen Maßnahmen

  Prüfungsgegenstand sind.

Wirtschaftsprüfungsstandards (Beispiel IDW PS 330)

- **Der IDW PS 330 ist ein Prüfungsstandard für Abschlussprüfungen beim Einsatz von Informationstechnologie.**

  Die Zielsetzung ist, zu beurteilen, ob das IT-gestützte Rechnungslegungssystem den gesetzlichen Anforderungen in Bezug auf Ordnungsmäßigkeit und Sicherheit entspricht. Er bezieht sich auf IT-gestützte Geschäftsprozesse, Anwendungen und IT-Infrastruktur, soweit sie rechnungslegungsrelevant sind.

UIMCert

Prüfung von rechnungsrelevanten Softwareprodukten nach PS 880

Die Prüfung bezieht sich im Einzelnen auf folgende Gebiete:

- Feststellung der notwendigen Verarbeitungsfunktion nach GoB,
- Prüfung der Richtigkeit der Programmabläufe und der programmierten Regeln zu den Verarbeitungsfunktionen,
- Prüfung der Softwaresicherheit,
- Prüfung der Verfahrensdokumentationen (System- und Anwenderdokumentationen).

UIMCert

Vorgehensweise bei der Durchführung von Audits

- **Zertifizierungsplan**

1. Festlegung der Zertifizierungsnorm
2. Zertifizierungs-Gegenstand
3. Zeitplanung bis zur Zertifikatserteilung
4. Umfang der Unterstützung durch externe Dienstleister
5. Umfang und Unterstützung durch Mitarbeiter
6. Projektaufwand und Budget
7. Fortschritt der internen Tätigkeit bis heute
8. Stufenplan der Projektdurchführung

Vorgehensweise bei der Durchführung von Audits

UIMCert

- **Vorgehensweise (Phasen):**

1. Auditierung der gelieferten Dokumentationen und Unterlagen
2. Vorbegutachtung dieser Dokumente
3. Prüfung der Funktionalitäten der Leistung/des verwendeten Verfahren
4. Erstellung eines Ergebnisberichtes der Funktionalitäts-/Verfahrensprüfung
5. Zusammenfassung der Dokumentations- und Funktionalitäts/Verfahrensprüfung
6. Auditierung der Ergebnisse der Dokumentenprüfung vor Ort
7. Durchsprache des gesamten Berichtes
8. Einbau eventueller aus der Durchsprache resultierender neuer Erkenntnisse
9. Vorlage des Berichtes bei der Zertifizierungsstelle
10. Ggfls. Beantwortung eventueller Rückfragen, u. U. nach Rücksprache mit dem Kunden
11. Ausfertigung des Gütesiegels/Zertifikates, Übernahme in die Gütesiegel/Zertifikatsliste

Tools als Hilfen bei der Prüfung

UIMCert

- **Das UIMCert-Prüftool als Hilfe**
  - Vorteile:
    Durchführen von strukturierten Analysen, speziell Unternehmens-, aber auch technische Analysen
  - Hochflexible Anpassung von analysen-/erhebungsbedingten Frageproblemen an die jeweiligen Erfordernisse
  - Rationelle computergestützte Erfassung von Erhebungsergebnissen und Antworten
  - Automatisierte Auswertung der Analyseergebnisse
  - Verbindung/Vernetzung von Antworten verschiedener Teilgebiete
  - Computergestützte Heraus-/Aufarbeitung von Schwachstellen
  - Zuordnung punktgenauer Maßnahmen zur Beseitigung der Schwachstellen
  - Rationalisierung der Arbeit durch „intelligente“ Textbausteine

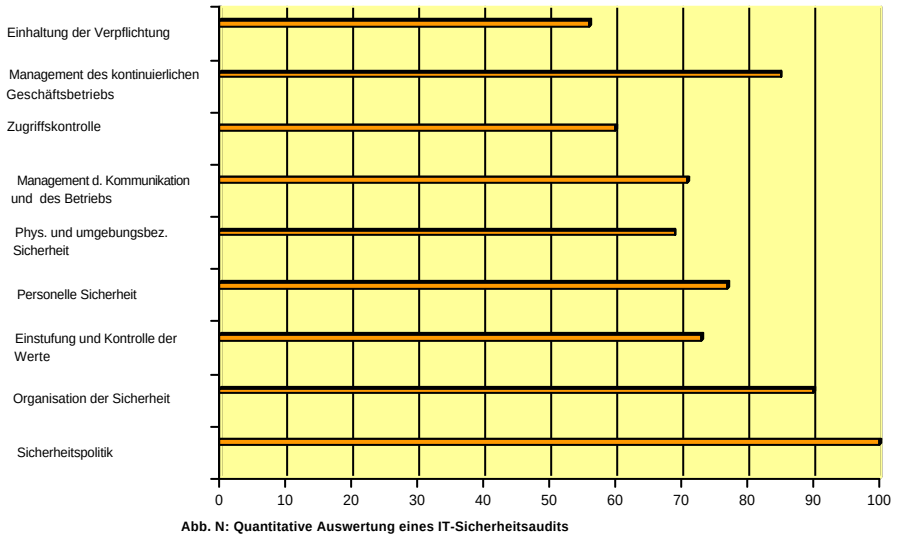
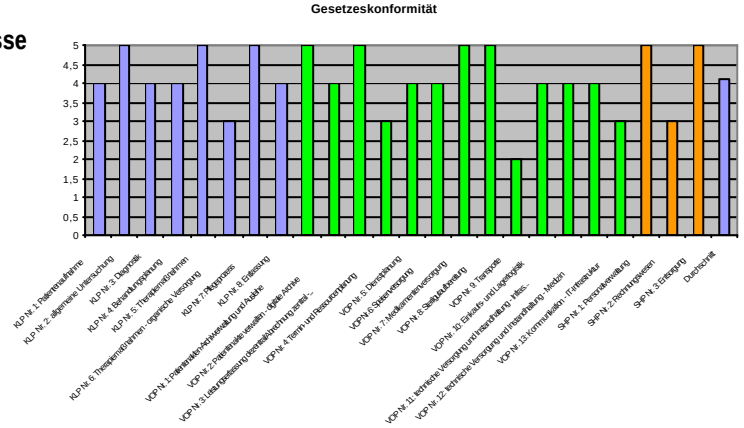


Abb. N: Quantitative Auswertung eines IT-Sicherheitsaudits

Toolgestützte Ergebnisse für das Management

- **Funktionsanalysen/Situationsanalysen**

Ergebnisse



Tools als Hilfen bei der Prüfung

UIMCert

- **Kriterien für die Auswahl von Tools**
  - Aufbau sollte den Prüfstandard widerspiegeln
  - Selbstklärende Fragen
  - Abstufung der Fragentiefe nach Relevanz
  - Verfeinerung der Fragen nach spezifischen Gegebenheiten des zu prüfenden Objektes
  - Automatische Auswertung und Berichtsgenerierung
  - Skalierbarkeit nach Unternehmensgröße, Branche, Userzahl
  - Mandantenfähigkeit nach Bewertungsobjekten
  - Fachlicher Support (Hotline für Fachfragen)
  - Referenzen und Empfehlungen durch Kunden oder Partner
  - Schulung/Einführung
  - Qualität der Software
  - Preis (Lizenz oder Kauf, Wartung, Preis-Leistungs-Verhältnis)

Fazit

UIMCert

- **Es gibt eine Vielzahl von Normen, Standards und gesetzlichen Regeln, die die Forderungen der 8. EU-Richtlinie präzisieren.**
- **Der Prüfer ist in der Lage, diese Normen und Standards zur Grundlage von Ordnungsmäßigkeitsprüfungen zu machen.**
- **Der Prüfer erhält hierdurch eine Prüfungsgrundlage, die nicht mehr diskutiert werden muss, die ihm hilft, Audits durchzuführen und Auditberichte zu erstellen.**
- **Es gibt eine Anzahl von Tools, die geeignet sind die Arbeit des Prüfers zu rationalisieren, zu strukturieren sowie die Berichterstellung zu erleichtern.**

Das Unternehmen

Geschäftsführer UIMCert: Prof. Dr. Reinhard Voßbein.
Gesellschafter: UIMC DR. Vossbein Betriebs-GmbH und Dr. Heiko Haaz
Die UIMCert GmbH ist eines der führenden Unternehmen im Bereich der Ordnungsmäßigkeitsprüfung und Zertifizierung bei IT-Sicherheit und Datenschutz.
Die UIMCert GmbH hat einen Fachbeirat, der die Geschäftsführung in wichtigen Fachfragen im Bereich IT-Sicherheit berät.
Die UIMCert GmbH verfügt über qualifiziertes Zertifizierungspersonal für die Begutachtung und Zertifizierung von Risikomanagement, IT-Sicherheit und Datenschutz.
Bei Bedarf Zusammenarbeit mit externen Stellen zur Ergänzung des eigenen Know-hows.
Weitere Geschäftsfelder: Aus- und Weiterbildung, Abwicklung von Forschungs- und Entwicklungsprojekten.

Seit dem 01.11.2001 ist die UIMCert GmbH als sachverständige Prüfstelle für den ISO 27001 / BS 7799 von der Trägergemeinschaft für Akkreditierung TGA akkreditiert.

Seit dem 01.02.2002 ist die UIMCert GmbH als erste sachverständige Prüfstelle in Deutschland gemäß § 3 Absatz 1 DSAVO für den Bereich Recht und Technik mit der fachlichen Spezialisierung im Bereich Datenschutzmanagement und -organisation vom ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein anerkannt.

Aufgaben / Aktivitäten der UIMCert

- Durchführung von Auditierungsprozessen und Ordnungsmäßigkeitsprüfungen
- Erteilen von Zertifikaten auf der Basis von Auditierungsergebnissen
- Kooperation mit anderen für andere Gebiete akkreditierten Unternehmen (z. B. ISO 9000)
- Begutachtung, Aufzeichnung und Überwachung der Kompetenz von Unterauftragnehmern.
- Bearbeitung von Anträgen auf Änderung des Geltungsbereichs der Zertifizierung

- Durchführung von Seminaren und Fortbildungsvorhaben.
- Abwicklung von Forschung- und Entwicklungsprojekten.