

Normen der IT-Sicherheit im Vergleich

DECUS IT Symposium 2005
Neuss, 2005-04-05

www.decus.de Peter Berlich, Martina Rohde

IT Symposium 20052005-04-05

Normen der IT-Sicherheit im Vergleich Inhalt

Einleitung

- Anlass und Motivation
- Begriffe und Ausgangssituation
- Übersicht und Aufbau
- Charakteristika von Sicherheitsmanagement**
- Zielsetzungen
- Verantwortlichkeiten
- Ausrichtung des Sicherheitsmanagements
- Anknüpfung an andere Managementbereiche
- Anknüpfung an andere Managementbereiche
- Anknüpfung an andere Managementbereiche
- Vergleich der Standards**
- ISO/IEC 17799 „Code of Practice for Information Security Management“
- Darstellung
- Bewertung
- ISO/IEC 13335 „Management of information and communications technology security“
- Darstellung
- Bewertung
- „IT-Grundsicherhandbuch“ (IT-GSHB) des BSI
- Darstellung
- Bewertung
- BS 7799-2 „Information Security Management Systems – Specification with Guidance for Use“
- Darstellung
- Bewertung
- Zusammenfassung und Ausblick**
- Literaturverzeichnis

- Einleitung
- Charakteristika von Sicherheitsmanagement
- Vergleich der Standards
 - ISO/IEC 17799 „Code of Practice for Information Security Management“
 - ISO/IEC 13335 „Management of information and communications technology security“
 - „IT-Grundsicherhandbuch“ (IT-GSHB) des BSI
 - BS 7799-2 „Information Security Management Systems – Specification with Guidance for Use“
- Zusammenfassung und Ausblick

www.decus.de Peter Berlich, Martina Rohde

IT Symposium 20052005-04-05

Normen der IT-Sicherheit im Vergleich

Einleitung

Einleitung

- Anlass und Motivation
- Begriffe und Ausgangssituation
- Übersicht und Aufbau

Charakteristika von Sicherheitsmanagement

- Bewertungsmerkmale
- Darstellungsmöglichkeiten
- Anpassung an Sicherheitsmanagement
- Ausrichtung des Sicherheitsmanagements
- Anlage im Sicherheitsmanagement

Vergleich der Standards

- ISO-IEC 17799 „Code of Practice for Information Security Management“
 - Darstellung
 - Bewertung
- ISO-IEC 15315 „Management of information and communications technology security“
 - Darstellung
 - Bewertung
- „IT-Grundschutzhandbuch“ (IT-CSS) des BSI
 - Darstellung
 - Bewertung
- BS 7799-2 „Information Security Management Systems – Specification with Guidance for Use“
 - Darstellung
 - Bewertung

Zusammenfassung und Ausblick

Literaturverzeichnis

- Anlass und Motivation
- Begriffe und Ausgangssituation
- Überblick und Aufbau

Normen der IT-Sicherheit im Vergleich

Anlass und Motivation

Einleitung

- Anlass und Motivation
- Begriffe und Ausgangssituation
- Übersicht und Aufbau

Charakteristika von Sicherheitsmanagement

- Bewertungsmerkmale
- Darstellungsmöglichkeiten
- Anpassung an Sicherheitsmanagement
- Ausrichtung des Sicherheitsmanagements
- Anlage im Sicherheitsmanagement

Vergleich der Standards

- ISO-IEC 17799 „Code of Practice for Information Security Management“
 - Darstellung
 - Bewertung
- ISO-IEC 15315 „Management of information and communications technology security“
 - Darstellung
 - Bewertung
- „IT-Grundschutzhandbuch“ (IT-CSS) des BSI
 - Darstellung
 - Bewertung
- BS 7799-2 „Information Security Management Systems – Specification with Guidance for Use“
 - Darstellung
 - Bewertung

Zusammenfassung und Ausblick

Literaturverzeichnis

- Normenvielfalt mündet in ein Auswahlproblem
- Zweckmässigkeit für die Ziele der Organisation (Überprüfbarkeit)
- Definition eines Klassifikationssystems für Sicherheitsmanagement-Standards

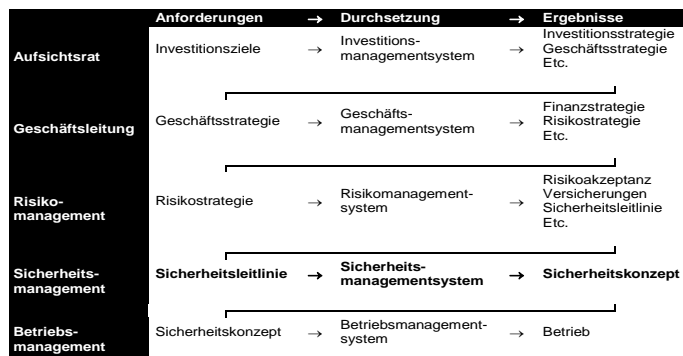
Normen der IT-Sicherheit im Vergleich Begriffe u. Ausgangssituation

Zusätzlich
Adress und Motivation
Begriffe und Ausgangssituation
 - Identifikation und Aufbau
 Charakteristika von Sicherheitsmanagementsystemen
 - Darstellungsmöglichkeiten
 - Anknüpfung an Sicherheitsmanagement
 - Anknüpfung des Sicherheitsmanagements
 - Anknüpfung im Sicherheitsmanagement
 Vergleich der Standards
 - ISO/IEC 17799 „Code of Practice for Information Security Management“
 - Darstellung
 - Bewertung
 - ISO/IEC 15315 „Management of Information and Communications Technology Security“
 - Darstellung
 - Bewertung
 - IT-Grundschutzhandbuch (IT-CSI) des BSI
 - Darstellung
 - Bewertung
 - BS 7799-2 „Information Security Management Systems – Specification with Guidance for Use“
 - Darstellung
 - Bewertung
 Zusammenfassung und Ausblick
 Literaturverzeichnis

- Sicherheitsmanagement
 - Ausgehend von einer maßvollen Zielvereinbarung wird mittels einer zielgerichteten Vorgehensweise ein sicherer Zielzustand angestrebt
 - Untermenge von Risikomanagement

Normen der IT-Sicherheit im Vergleich Begriffe u. Ausgangssituation

Zusätzlich
Adress und Motivation
Begriffe und Ausgangssituation
 - Identifikation und Aufbau
 Charakteristika von Sicherheitsmanagementsystemen
 - Darstellungsmöglichkeiten
 - Anknüpfung an Sicherheitsmanagement
 - Anknüpfung des Sicherheitsmanagements
 - Anknüpfung im Sicherheitsmanagement
 Vergleich der Standards
 - ISO/IEC 17799 „Code of Practice for Information Security Management“
 - Darstellung
 - Bewertung
 - ISO/IEC 15315 „Management of Information and Communications Technology Security“
 - Darstellung
 - Bewertung
 - IT-Grundschutzhandbuch (IT-CSI) des BSI
 - Darstellung
 - Bewertung
 - BS 7799-2 „Information Security Management Systems – Specification with Guidance for Use“
 - Darstellung
 - Bewertung
 Zusammenfassung und Ausblick
 Literaturverzeichnis



Normen der IT-Sicherheit im Vergleich Begriffe u. Ausgangssituation

Zielsetzung
 - Anlass und Motivation
 - Begriffe und Ausgangssituation
 - Überblick und Aufbau

Charakteristika von Sicherheitsmanagementsystemen
 - Die Zielsetzungen
 - Besondere Merkmale
 - Ausprägung im Sicherheitsmanagement
 - Anordnung des Sicherheitsmanagements
 - Anknüpfung an das Sicherheitsmanagement

Vergleich der Standards
 - ISO/IEC 17799: Code of Practice for Information Security Management
 - Darstellung
 - Bewertung
 - ISO/IEC 15335: Management of information and communications technology security
 - Darstellung
 - Bewertung
 - IT-Grundschutzhandbuch (IT-Grundschutz)
 - Darstellung
 - Bewertung
 - BS 7799-2: Information Security Management Systems – Specification with Guidance for Use
 - Darstellung
 - Bewertung
 - Zusammenfassung und Ausblick
 - Literaturverzeichnis

- Kernfragen des Anwenders
 - Welche Aktivitäten sind in welcher Reihenfolge mit welchen Arbeitsergebnissen durchzuführen?
 - Wodurch ist ein sicherer Zielzustand gekennzeichnet?
 - Wie kann das einer gegebenen Situation angemessene Sicherheitsniveau bestimmt werden?

Normen der IT-Sicherheit im Vergleich Überblick und Aufbau

Zielsetzung
 - Anlass und Motivation
 - Begriffe und Ausgangssituation
 - Überblick und Aufbau

Charakteristika von Sicherheitsmanagementsystemen
 - Die Zielsetzungen
 - Besondere Merkmale
 - Ausprägung im Sicherheitsmanagement
 - Anordnung des Sicherheitsmanagements
 - Anknüpfung an das Sicherheitsmanagement

Vergleich der Standards
 - ISO/IEC 17799: Code of Practice for Information Security Management
 - Darstellung
 - Bewertung
 - ISO/IEC 15335: Management of information and communications technology security
 - Darstellung
 - Bewertung
 - IT-Grundschutzhandbuch (IT-Grundschutz)
 - Darstellung
 - Bewertung
 - BS 7799-2: Information Security Management Systems – Specification with Guidance for Use
 - Darstellung
 - Bewertung
 - Zusammenfassung und Ausblick
 - Literaturverzeichnis

- Basierend auf der Bedürfnisabschätzung des Anwenders
 - Welcher Standard wird dem **Problem** des Anwenders gerecht?
 - Die Anwendung welchen Standards unterstützt die **Intention** des Anwenders?
 - Definition geeigneter Charakteristika
 - Darstellung und Bewertung der Standards.

Normen der IT-Sicherheit im Vergleich Charakteristika

Zielsetzung
 - Adress und Motivation
 - Begriffs und Abgrenzung
 - Umfang und Aufbau
Charakteristika von
Sicherheitsmanagements
 - Darstellungselemente
 - Bewertungskriterien
 - Ausprägung im
 - Sicherheitsmanagement
 - Ausrichtung des
 - Sicherheitsmanagements
 - Aussage im
 - Sicherheitsmanagement
Vergleich der Standards
 - ISO-IEC 17799 „Code of Practice
 for Information Security
 Management“
 - Darstellung
 - Bewertung
 - ISO-IEC 15335 „Management of
 information and communications
 technology security“
 - Darstellung
 - Bewertung
 - IT-Grundschutzhandbuch (IT-
 CS) des BSI
 - Darstellung
 - Bewertung
 - BS 7799-2 „Information Security
 Management Systems –
 Specification with Guidance for Use“
 - Darstellung
 - Bewertung
 - Zusammenfassung und Ausblick
 - Literaturverzeichnis

- Darstellungsmerkmale
- Bewertungskriterien
- Ausprägung im Sicherheitsmanagement
- Ausrichtung des Sicherheitsmanagements
- Aussage im Sicherheitsmanagement

Normen der IT-Sicherheit im Vergleich Darstellungsmerkmale

Zielsetzung
 - Adress und Motivation
 - Begriffs und Abgrenzung
 - Umfang und Aufbau
Charakteristika von
Sicherheitsmanagements
 - Darstellungselemente
 - Bewertungskriterien
 - Ausprägung im
 - Sicherheitsmanagement
 - Ausrichtung des
 - Sicherheitsmanagements
 - Aussage im
 - Sicherheitsmanagement
Vergleich der Standards
 - ISO-IEC 17799 „Code of Practice
 for Information Security
 Management“
 - Darstellung
 - Bewertung
 - ISO-IEC 15335 „Management of
 information and communications
 technology security“
 - Darstellung
 - Bewertung
 - IT-Grundschutzhandbuch (IT-
 CS) des BSI
 - Darstellung
 - Bewertung
 - BS 7799-2 „Information Security
 Management Systems –
 Specification with Guidance for Use“
 - Darstellung
 - Bewertung
 - Zusammenfassung und Ausblick
 - Literaturverzeichnis

- Problemadäquanz (Wird der Standard dem Problem des Anwenders gerecht?)
- Zielsetzung und -gruppe
 - Geschäftsleitung (Senior Management)
 - Sicherheits-Beauftragter (Security Officer)
 - Sicherheits-Administrator
- Form und Inhalt
 - Detaillierungsgrad (entsprechend: Verfeinerungsaufwand)
 - Gütesiegel auf basis existierender Zertifizierungsschemata?

Normen der IT-Sicherheit im Vergleich

Bewertungskriterien

Inhaltung

- Adress und Motivation
- Begriffe und Abgrenzungen
- Umfeld und Aufbau
- Charakteristika von Sicherheitsmanagements
- Die Handlungsmerkmale
- Beurteilungsmerkmale
- Ausprägung im Sicherheitsmanagements
- Ausrichtung des Sicherheitsmanagements
- Anlage im Sicherheitsmanagements
- Vergleich der Standards
- ISO-IEC 17799 'Code of Practice for Information Security Management'
- Darstellung
- Bewertung
- ISO-IEC 15315 'Management of information and communications technology security'
- Darstellung
- Bewertung
- 'IT-Grundschutzhandbuch' (IT-CSS) des BSI
- Darstellung
- Bewertung
- BS 7799-2 'Information Security Management Systems - Specification with Guidance for Use'
- Darstellung
- Bewertung
- Zusammenfassung und Ausblick
- Literaturverzeichnis

- Zur Entscheidung, inwieweit die **Anwendung des Standards die Absicht des Anwenders unterstützt (Intentionsorientierung)**, werden innere, inhaltliche Merkmale heran gezogen.

Normen der IT-Sicherheit im Vergleich

Ausprägung

Inhaltung

- Adress und Motivation
- Begriffe und Abgrenzungen
- Umfeld und Aufbau
- Charakteristika von Sicherheitsmanagements
- Die Handlungsmerkmale
- Beurteilungsmerkmale
- Ausprägung im Sicherheitsmanagements
- Ausrichtung des Sicherheitsmanagements
- Anlage im Sicherheitsmanagements
- Vergleich der Standards
- ISO-IEC 17799 'Code of Practice for Information Security Management'
- Darstellung
- Bewertung
- ISO-IEC 15315 'Management of information and communications technology security'
- Darstellung
- Bewertung
- 'IT-Grundschutzhandbuch' (IT-CSS) des BSI
- Darstellung
- Bewertung
- BS 7799-2 'Information Security Management Systems - Specification with Guidance for Use'
- Darstellung
- Bewertung
- Zusammenfassung und Ausblick
- Literaturverzeichnis

- Sicherheitsmanagementprozess unterteilt in
 - Planung
 - Durchführung
 - Kontrolle
- Sicherheitsmanagementsystem
 - Ziele/ Metriken
 - organisatorische Prinzipien/ Rollen
 - Mitarbeiter/ Ressourcen
- **Ausprägung**
 - **Prozedural**
 - **Systemisch**

Normen der IT-Sicherheit im Vergleich

Ausrichtung

Zielsetzung

- Adress und Motivation
- Begriffe und Angewandtheiten
- Umfeld und Aufbau

Charakteristika von

- Sicherheitsmanagement
- Die Handlungsmerkmale
- Beurteilungsmerkmale
- Ausprägung des
- Sicherheitsmanagements
- Ausrichtung des
- Sicherheitsmanagements
- Ansatz im
- Sicherheitsmanagement

Vergleich der Standards

- ISO-IEC 17799 „Code of Practice for Information Security Management“
- Darstellung
- Bewertung
- ISO-IEC 15335 „Management of information and communications technology security“
- Darstellung
- Bewertung
- „IT-Grundschutzhandbuch“ (IT-CSS) des BSI
- Darstellung
- Bewertung
- BS 7799-2 „Information Security Management Systems – Specification with Guidance for Use“
- Darstellung
- Bewertung

Zusammenfassung und Ausblick

- Literaturverzeichnis

- Kriterien eines technischen oder organisatorischen Systems hinsichtlich seiner
 - Funktionalität
 - Implementierungsqualität
- **Ausrichtung**
 - Sicherheitsbildend
 - Vertrauensbildend

www.decus.de Peter Berlich, Martina Rohde

IT Symposium 2005/2005-04-05

Normen der IT-Sicherheit im Vergleich

Aussage

Zielsetzung

- Adress und Motivation
- Begriffe und Angewandtheiten
- Umfeld und Aufbau

Charakteristika von

- Sicherheitsmanagement
- Die Handlungsmerkmale
- Beurteilungsmerkmale
- Ausprägung des
- Sicherheitsmanagements
- Ausrichtung des
- Sicherheitsmanagements
- Ansatz im
- Sicherheitsmanagement

Vergleich der Standards

- ISO-IEC 17799 „Code of Practice for Information Security Management“
- Darstellung
- Bewertung
- ISO-IEC 15335 „Management of information and communications technology security“
- Darstellung
- Bewertung
- „IT-Grundschutzhandbuch“ (IT-CSS) des BSI
- Darstellung
- Bewertung
- BS 7799-2 „Information Security Management Systems – Specification with Guidance for Use“
- Darstellung
- Bewertung

Zusammenfassung und Ausblick

- Literaturverzeichnis

- Das Sicherheitsniveau ist angemessen, wenn die Sicherheitsrichtlinie die Geschäftsziele widerspiegelt und angemessen umgesetzt wird.
- **Überprüfungsfähigkeit** hinsichtlich
 - **Conformance** (Befolgung der dokumentierten Vorgehensweisen)
 - **Compliance** (Befolgung der Sicherheitsmassnahmen)
 - **Capability/ Maturity** (Nachhaltigkeit, langfristige Erreichbarkeit der Sicherheitsziele)

www.decus.de Peter Berlich, Martina Rohde

IT Symposium 2005/2005-04-05

Normen der IT-Sicherheit im Vergleich

Vergleich der Standards

Zielsetzung

- Adress und Motivation
- Begriffe und Abgrenzungen
- Umfeld und Aufbau
- Charakteristika von Sicherheitsmanagement
- Die Handlungsmerkmale
- Maßnahmenbereiche
- Anpassung an
- Sicherheitsmanagement
- Ausrichtung des
- Sicherheitsmanagements
- Ansatz im
- Sicherheitsmanagement

Vergleich der Standards

- ISO/IEC 17799 „Code of Practice for Information Security Management“
- Darstellung
- Bewertung
- ISO/IEC 13335 „Management of information and communications technology security“
- Darstellung
- Bewertung
- „IT-Grundschutzhandbuch“ (IT-GSHB) des BSI
- Darstellung
- Bewertung
- BS 7799-2 „Information Security Management Systems – Specification with Guidance for Use“
- Darstellung
- Bewertung
- Zusammenfassung und Ausblick
- Literaturverzeichnis

- ISO/IEC 17799 „Code of Practice for Information Security Management“
- ISO/IEC 13335 „Management of information and communications technology security“
- „IT-Grundschutzhandbuch“ (IT-GSHB) des BSI
- BS 7799-2 „Information Security Management Systems – Specification with Guidance for Use“

www.decus.dePeter Berlich, Martina Rohde

IT Symposium 20052005-04-05

Normen der IT-Sicherheit im Vergleich

ISO/IEC 17799: Darstellung

Zielsetzung

- Adress und Motivation
- Begriffe und Abgrenzungen
- Umfeld und Aufbau
- Charakteristika von Sicherheitsmanagement
- Die Handlungsmerkmale
- Maßnahmenbereiche
- Anpassung an
- Sicherheitsmanagement
- Ausrichtung des
- Sicherheitsmanagements
- Ansatz im
- Sicherheitsmanagement

Vergleich der Standards

- ISO/IEC 17799 „Code of Practice for Information Security Management“
- Darstellung
- Bewertung
- ISO/IEC 13335 „Management of information and communications technology security“
- Darstellung
- Bewertung
- „IT-Grundschutzhandbuch“ (IT-GSHB) des BSI
- Darstellung
- Bewertung
- BS 7799-2 „Information Security Management Systems – Specification with Guidance for Use“
- Darstellung
- Bewertung
- Zusammenfassung und Ausblick
- Literaturverzeichnis

- Zielsetzung und -gruppe
 - Darstellung von Informationssicherheit als Gesamtaufgabe darzustellen
 - Es dient dem „Managen“ von Sicherheit in einer Organisation, indem es einzelne Teilaufgaben beschreibt.
 - Das Dokument richtet sich an Sicherheits-Beauftragte.
- Form und Inhalt
 - Im Dokument [17799] sind mehrere Maßnahmenbereiche (Control areas) aufgeführt: Sicherheitsleitlinie, Organisation, Asset Management, Personal, Infrastruktur, Netzwerk- und Systemmanagement, Zugriffskontrolle, Systembeschaffung, entwicklung und wartung, Behandlung von Sicherheitsvorfällen, Notfallvorsorge und Compliance.
 - Das Dokument listet die Maßnahmenbereiche (in ungeordneter Reihenfolge und ohne Priorität) auf. Es ist nicht detailliert genug, um der Zielgruppe als unmittelbare Handreichung zu dienen.
 - Die Implementierungshilfen zu den einzelnen Maßnahmen müssen im Anwendungsfall erweitert bzw. verfeinert werden.
 - Das Dokument hat demnach einen mittleren Detaillierungsgrad.

www.decus.dePeter Berlich, Martina Rohde

IT Symposium 20052005-04-05

Normen der IT-Sicherheit im Vergleich ISO/IEC 17799: Bewertung

Zielsetzung

- Adress und Motivation
- Begriffe und Angewandtheit
- Umfang und Aufbau
- Charakteristika von Sicherheitsmanagements
- Darstellungsmarkende
- Beziehungsmerkmale
- Angewandtheit
- Ausrichtung des Sicherheitsmanagements
- Anlage im Sicherheitsmanagement
- Vergleich der Standards
- ISO/IEC 17799: „Code of Practice for Information Security Management“
- Darstellung
- Bewertung
- ISO/IEC 13335: „Management of information and communications technology security“
- Darstellung
- Bewertung
- IT-Grundschutzhandbuch (IT-CSI) des BSI
- Darstellung
- Bewertung
- ISO 27001-2 „Information Security Management Systems – Specifications with Guidance for Use“
- Darstellung
- Bewertung
- Zusammenfassung und Ausblick
- Literaturverzeichnis

- Ausprägung**
 - Der Fokus des Maßnahmenbereichs „Organizing information security“ liegt eher auf dem systemischen Aspekt.
 - Das neue Kapitel „Risk assessment and treatment“ fokussiert eher prozedurale Aspekte.
- Ausrichtung**
 - Vertrauensbildende Aspekte sind an einigen Stellen erwähnt; so wird „Risk assessment and treatment“ ein ganzes Kapitel gewidmet.
 - Schwerpunktmäßig werden aber sicherheitsbildende Aspekte behandelt.
- Aussage**
 - Der Sicherheitsleitlinie wird ein eigener Maßnahmenbereich „Security policy“ gewidmet. In der Sicherheitsmaßnahme „Independent review of information security“ wird die Wichtigkeit des Überprüfens von Managementansatz und Maßnahmenimplementierung betont.
 - Das Dokument selbst ist nicht unmittelbar verwendbar, um eine Compliance-Prüfung durchzuführen. Es kann lediglich zur Konformitäts-Prüfung, ob alle Maßnahmenbereiche abgedeckt sind, herangezogen werden.
 - Eine Capability/ Maturity-Prüfung ist mit dem Dokument nicht möglich.

www.decus.dePeter Berlich, Martina Rohde

IT Symposium 20052005-04-05

Normen der IT-Sicherheit im Vergleich ISO/IEC 13335: Darstellung

Zielsetzung

- Adress und Motivation
- Begriffe und Angewandtheit
- Umfang und Aufbau
- Charakteristika von Sicherheitsmanagements
- Darstellungsmarkende
- Beziehungsmerkmale
- Angewandtheit
- Ausrichtung des Sicherheitsmanagements
- Anlage im Sicherheitsmanagement
- Vergleich der Standards
- ISO/IEC 17799: „Code of Practice for Information Security Management“
- Darstellung
- Bewertung
- ISO/IEC 13335: „Management of information and communications technology security“
- Darstellung
- Bewertung
- IT-Grundschutzhandbuch (IT-CSI) des BSI
- Darstellung
- Bewertung
- ISO 27001-2 „Information Security Management Systems – Specifications with Guidance for Use“
- Darstellung
- Bewertung
- Zusammenfassung und Ausblick
- Literaturverzeichnis

- Zielsetzung und -gruppe**
 - Ziel der Dokumente ist es, Informations- und Kommunikations-Sicherheit als einen Prozess von Planen, Umsetzen und Betreiben darzustellen.
 - Beide dienen damit dem „Managen“ von Sicherheit in einer Organisation.
 - Beide Dokumente richteten sich an – Sicherheits-Beauftragte.
- Form und Inhalt**
 - Im Teil 1 werden sicherheitsrelevante Begriffe wie u. a. Werte, Bedrohungen, Schwachstellen, Schäden, Risiken, Sicherheitsmaßnahmen und deren Beziehung zueinander sowie Ziele, Strategien und Leitlinien vorgestellt.
 - Neben organisatorischen Aspekten wie z. B. Rollen und Zuständigkeiten werden auch Sicherheitsmanagement-Funktionen angedrungen sowie die Notwendigkeit von Risikomanagement betont. Im Teil 2 [N3951] wird der Risikomanagement-Prozess dargestellt.
 - Die Aktivitäten der Risikobewertung werden detailliert beschrieben. Weitere Sicherheitsmanagement-Funktionen werden dem Risikomanagement-Prozess zugeordnet.
 - Ein großer Teil des Anhangs beschreibt, wie bei der Auswahl von Sicherheitsmaßnahmen vorzugehen ist.
 - Beide Dokumente sind detailliert genug, um der Zielgruppe als Handreichung, nicht jedoch als Verfahrens- bzw. Arbeitsanweisung zu dienen. Das Dokument hat demnach einen mittleren Detaillierungsgrad.

www.decus.dePeter Berlich, Martina Rohde

IT Symposium 20052005-04-05

Normen der IT-Sicherheit im Vergleich ISO/IEC 13335: Bewertung

Zielsetzung
 - Anlass und Motivation
 - Begriffe und Abgrenzungen
 - Übersicht und Aufbau
Charakteristika von
 - Sicherheitsmanagement
 - Die Handlungsmerkmale
 - Risikomanagement
 - Ausprägung im
 - Schriftlichmanagement
 - Ausrichtung des
 - Schriftlichmanagement
 - Ansatz im
 - Schriftlichmanagement
Vergleich der Standards
 - ISO/IEC 17799 „Code of Practice
 for Information Security
 Management“
 - Darstellung
 - Bewertung
 - ISO/IEC 15335 „Management of
 information and communications
 technology security“
 - Darstellung
 - Bewertung
 - IT-Grundschutzhandbuch (IT-
 GSHB) des BSI
 - Darstellung
 - Bewertung
 - BS 7799-2 „Information Security
 Management Systems –
 Specification with Guidance for Use“
 - Darstellung
 - Bewertung
Zusammenfassung und Ausblick
 - Literaturverzeichnis

- **Ausprägung**
 - Der Risikomanagement-Prozess ist prozessorientiert; die organisatorischen Grundsätze sind systemorientiert.
 - Beide Dokumente zusammen sind sowohl prozedural als auch systemisch ausgeprägt.
- **Ausrichtung**
 - In Teil 1 werden schwerpunktmäßig sicherheitsbildende Aspekte behandelt.
 - Die Risikobewertung in Teil 2 ist eher ein vertrauensbildender Aspekt; die Maßnahmenauswahl in Teil 2 ist eher ein sicherheitsbildender Aspekt.
- **Aussage**
 - Beide Dokumente selbst sind nicht unmittelbar verwendbar, um eine Compliance-Prüfung durchzuführen.
 - Sie können lediglich zur Konformitäts-Prüfung herangezogen werden.
 - Eine Capability/ Maturity-Prüfung ist mit dem Dokument nicht möglich.

www.decus.de Peter Berlich, Martina Rohde

IT Symposium 2005/2005-
04-05

Normen der IT-Sicherheit im Vergleich IT-GSHB: Darstellung

Zielsetzung
 - Anlass und Motivation
 - Begriffe und Abgrenzungen
 - Übersicht und Aufbau
Charakteristika von
 - Sicherheitsmanagement
 - Die Handlungsmerkmale
 - Risikomanagement
 - Ausprägung im
 - Schriftlichmanagement
 - Ausrichtung des
 - Schriftlichmanagement
 - Ansatz im
 - Schriftlichmanagement
Vergleich der Standards
 - ISO/IEC 17799 „Code of Practice
 for Information Security
 Management“
 - Darstellung
 - Bewertung
 - ISO/IEC 15335 „Management of
 information and communications
 technology security“
 - Darstellung
 - Bewertung
 - IT-Grundschutzhandbuch (IT-
 GSHB) des BSI
 - Darstellung
 - Bewertung
 - BS 7799-2 „Information Security
 Management Systems –
 Specification with Guidance for Use“
 - Darstellung
 - Bewertung
Zusammenfassung und Ausblick
 - Literaturverzeichnis

- **Zielsetzung und -gruppe**
 - Ziel des Dokumentes ist es, durch ausgewählte Sicherheitsmaßnahmen ein Mindest-Sicherheitsniveau für IT-Systeme vorzugeben.
 - Es dient somit dem Management von Sicherheit in einer Organisation, indem es die einzelnen Aktivitäten und Maßnahmen – also das „Wie“ und „Womit“ – beschreibt.
 - Das Dokument behandelt Informations- und Kommunikations-Sicherheit und richtet sich an die Sicherheits-Beauftragte und Administratoren, weniger an die Geschäftsleitung.
- **Form und Inhalt**
 - Neben einer Beschreibung zur Anwendung des Handbuchs findet sich eine Vielzahl von so genannten „Bausteinen“ bezogen auf bestimmte IT-Systeme.
 - Darüberhinaus enthält das Dokument Maßnahmenkataloge sowie zusätzlich hierzu Gefährdungskataloge.
 - Die Beschreibung ist detailliert genug, um der Zielgruppe als Verfahrens- bzw. Arbeitsanweisung zu dienen.
 - Sowohl die generischen als auch die produkt-/ technologiespezifischen Sicherheitsmaßnahmen sind erläutert und auf den Anwendungsfall direkt übertragbar.
 - Das Dokument hat demnach einen hohen Detaillierungsgrad.
 - Aufbauend auf dem IT-GSHB wird vom BSI ein Auditierungs- und Zertifizierungsschema definiert.

www.decus.de Peter Berlich, Martina Rohde

IT Symposium 2005/2005-
04-05

Normen der IT-Sicherheit im Vergleich BS 7799-2: Bewertung

Einführung	Adress und Motivation Begriffe und Angewandtheiten Umfeld und Aufbau
Charakteristika von Sicherheitsmanagementsystemen	Charakteristika von Sicherheitsmanagementsystemen Die Handlungsmerkmale Bewertungsmerkmale Ausprägung im Sicherheitsmanagementsystem Ausrichtung des Sicherheitsmanagements Anlage im Sicherheitsmanagementsystem
Vergleich der Standards	BS-ISO 17799: Code of Practice for Information Security Management Darstellung Bewertung ISO-IEC 15333: Management of information and communications technology security Darstellung Bewertung IT-Grundschutzhandbuch IT-CSSM des BSI Darstellung Bewertung BS 7799-2: Information Security Management System Spezifikation with Guidance for Use Darstellung Bewertung
Zusammenfassung und Ausblick	Zusammenfassung und Ausblick Literaturverzeichnis

- **Ausprägung**
 - Die einzelnen Prozess-Aktivitäten werden nur dargelegt und nicht beschrieben. Die Elemente des Managementsystems werden dargelegt.
 - Der Fokus ist systemisch.
- **Ausrichtung**
 - Der Dokumentation ist ein eigenes Kapitel „Documentation requirements“ gewidmet. Auch wird auf die „Management responsibility“ verwiesen.
 - Schwerpunktmäßig werden aber vertrauensbildende Aspekte behandelt.
- **Aussage**
 - Das Dokument ist nicht verwendbar, um eine Compliance-Prüfung durchzuführen.
 - Es kann lediglich zur Konformitäts-Prüfung herangezogen werden.
 - Da im Dokument selbst keine Metrik enthalten ist, mit der überprüft werden kann, ob ein Systemelement erfüllt ist oder nicht, kann es für sich genommen auch nicht als Basis für eine Capability/ Maturity-Prüfung herangezogen werden.

www.decus.dePeter Berlich, Martina Rohde

IT Symposium 20052005-04-05

Normen der IT-Sicherheit im Vergleich Zusammenfassung & Ausblick

Einführung	Adress und Motivation Begriffe und Angewandtheiten Umfeld und Aufbau
Charakteristika von Sicherheitsmanagementsystemen	Charakteristika von Sicherheitsmanagementsystemen Die Handlungsmerkmale Bewertungsmerkmale Ausprägung im Sicherheitsmanagementsystem Ausrichtung des Sicherheitsmanagements Anlage im Sicherheitsmanagementsystem
Vergleich der Standards	BS-ISO 17799: Code of Practice for Information Security Management Darstellung Bewertung ISO-IEC 15333: Management of information and communications technology security Darstellung Bewertung IT-Grundschutzhandbuch IT-CSSM des BSI Darstellung Bewertung BS 7799-2: Information Security Management System Spezifikation with Guidance for Use Darstellung Bewertung
Zusammenfassung und Ausblick	Zusammenfassung und Ausblick Literaturverzeichnis

- Einführung eines ISMS kann z. Z. beispielsweise basierend auf BS7799-2 erfolgen
- Der SM-Prozess kann dann auf der Grundlage eines (mehr oder minder unmittelbar anwendbaren Standards) erfolgen.
- Als Schwäche tritt bei allen Standards eine Unschärfe der Ausprägung von Prozess- oder Systemsicht zu Tage.
- Keiner der Standards unterscheidet explizit zwischen sicherheits- und vertrauensbildenden Maßnahmen. Nur bei einem der vorgestellten Standards eine entsprechende Metrik definiert.
- Wer einen Überblick über relevante Maßnahmenbereiche sucht, der ist mit IS 17799 gut bedient. Für die Vorgehensweise beim „Managen“ von Sicherheit wissen sollte IS 13335 zu Rate gezogen werden.
- Im Gegensatz zu den beiden vorangestellten liefert das IT-GSHB konkrete Anleitungen/Massnahmen.
- BS 7799-2 hingegen befasst sich nicht mit Sicherheit an sich, sondern mit dem umgebenden Managementsystem.

www.decus.dePeter Berlich, Martina Rohde

IT Symposium 20052005-04-05

Normen der IT-Sicherheit im Vergleich Zusammenfassung & Ausblick

Einleitung
 Anlass und Motivation
 Begriffs- und Abgrenzungen
 Übersicht und Aufbau
 Charakteristika von
 Sicherheitsmanagementsystemen
 Darstellungsmethoden
 Bewertungsmethoden
 Ausprägung im
 Schriftlichem Management
 Ausrichtung des
 Schriftlichem Managements
 Anknüpfung an
 Schriftlichem Management
 Vergleich der Standards
 BSI-ISO 17799 „Code of Practice
 for Information Security
 Management“
 Darstellung
 Bewertung
 ISO-IEC 15333 „Management of
 information and communications
 technology security“
 Darstellung
 Bewertung
 IT-Grundschutzhandbuch IT-
 CS 101 des BSI
 Darstellung
 Bewertung
 BS 7799-2 „Information Security
 Management Systems –
 Specifications with Guidance for Use“
 Darstellung
 Bewertung
 Zusammenfassung und Ausblick
 Literaturverzeichnis

	Untersuchungs- gegenstand	Zielgruppe	Detaillierungs- grad	Gütesiegel
IS 17799	Informations- Sicherheit	Beauftragter	mittel	Nein
IS 13335	Informations- und Kommunikations- Sicherheit*	Beauftragter	mittel	Nein
BSI IT-GSHB	Informations- und Kommunikations- Sicherheit*	Beauftragter/ Administrator	hoch	Ja
BS 7799-2	Informations- Sicherheit	Geschäfts- leitung	niedrig	Ja
	Ausprägung	Ausrichtung	Aussage	
IS 17799	Prozess/ System	Funktionalität	Befolgung	
IS 13335	Prozess/ System	Funktionalität/ Implementierungs- qualität	Befolgung	
BSI IT-GSHB	Prozess/ System	Funktionalität/ Implementierungs- qualität	Übereinstimmung / Befolgung	
BS 7799-2	System	Implementierungs- qualität	Befolgung	

www.decus.de Peter Berlich, Martina Rohde

IT Symposium 2005/2005-
04-05

Normen der IT-Sicherheit im Vergleich Zusammenfassung & Ausblick

Einleitung
 Anlass und Motivation
 Begriffs- und Abgrenzungen
 Übersicht und Aufbau
 Charakteristika von
 Sicherheitsmanagementsystemen
 Darstellungsmethoden
 Bewertungsmethoden
 Ausprägung im
 Schriftlichem Management
 Ausrichtung des
 Schriftlichem Managements
 Anknüpfung an
 Schriftlichem Management
 Vergleich der Standards
 BSI-ISO 17799 „Code of Practice
 for Information Security
 Management“
 Darstellung
 Bewertung
 ISO-IEC 15333 „Management of
 information and communications
 technology security“
 Darstellung
 Bewertung
 IT-Grundschutzhandbuch IT-
 CS 101 des BSI
 Darstellung
 Bewertung
 BS 7799-2 „Information Security
 Management Systems –
 Specifications with Guidance for Use“
 Darstellung
 Bewertung
 Zusammenfassung und Ausblick
 Literaturverzeichnis

- Das vorgestellte Klassifikationssystem ermöglicht eine Einordnung von Sicherheitsmanagement-Standards.
- Insbesondere wird offensichtlich, dass es zurzeit keine vollständige Liste aller relevanten Prozessaktivitäten und Systemelemente gibt.
- Erst anhand dieser Listen wäre eine Aussage über den Abdeckungsgrad von Standards möglich.
- Insbesondere in Bezug auf eine Aussagefähigkeit über das erreichte Sicherheitsniveau weisen (fast) alle untersuchten Standards noch erhebliche Schwächen auf.
- Es sei an dieser Stelle darauf hingewiesen, dass es umfangreiche Sammlungen von Best Practices gibt, die eine detaillierte Aussage über das erreichte Sicherheitsniveau ermöglichen.

www.decus.de Peter Berlich, Martina Rohde

IT Symposium 2005/2005-
04-05

Normen der IT-Sicherheit im Vergleich Literaturverzeichnis

Einleitung

Adress und Motivation

Begriffe und Ausgangssituation

Übersicht und Aufbau

Charakteristika von

Sicherheitsmanagementsystemen

Die Abstammungserkennung

Beurteilungskriterien

Anpassung an

Sicherheitsmanagement

Ausrichtung des

Sicherheitsmanagements

Ansatz im

Sicherheitsmanagement

Vergleich der Standards

ISO/IEC 17799: Code of Practice for Information Security Management

Beurteilung

ISO/IEC 13335: Management of information and communications technology security

Beurteilung

BS 7799-2: Information Security Management Systems - Specifications with Guidance for Use

Beurteilung

Zusammenfassung und Ausblick

Literaturverzeichnis

- BSI: Studie zu ISO-Normungsaktivitäten ISO/BPM - Vergleich der Audit- und Zertifizierungsschemata für IT-Grundschutz und BS 7799-2. http://www.bsi.bund.de/literat/studien/gshb/ISO-BPM-Zertifizierung_040305.pdf, download 2004-06-29.
- BSI: Studie zu ISO-Normungsaktivitäten ISO/BPM - Anforderungen an Information Security Management Systeme. http://www.bsi.bund.de/literat/studien/gshb/ISO-BPM-IMS_040305.pdf, download 2004-06-29.
- van Essen, U. (Hrsg.): Sicherheit des Betriebssystems VMS. Studien des BSI, Band 4, Oldenburg Verlag, München, 1991.
- D21-Initiative: IT-Sicherheitskriterien im Vergleich. http://www.initiative21.de/druck/news/publikationen2002/doc/22_1053502380.pdf.
- BSI: IT-Grundschutz-Handbuch. <http://www.bsi.bund.de/gshb/deutsch/etc/titel.htm>, download 2004-06-29.
- Heschl, J.: COBIT in Relation to Other International Standards. Information Systems Control Journal, Vol. 4/2004.
- Hill, W., Fehlbaum, U., Ulrich, P. Organisationslehre 1. Paul Haupt Verlag, Bern, 1989.
- Hill, W., Fehlbaum, U., Ulrich, P. Organisationslehre 2. Paul Haupt Verlag, Bern, 1992.
- ISF: Forum Standard of Good Practice. ISF. http://www.isfsecuritystandard.com/index_ie.htm, download 2004-06-29.
- Kieser, A., Kubicek, H.: Organisation. de Gruyter Verlag, Berlin, 1992.
- Expert contribution on "Application of the CC to ISMS, Feasibility Study."
- ISO/IEC 13335-1: Information technology - Security techniques - Management of information and communications technology security (MICTS) - Part 1: Concepts and models for managing and planning ICT security. Text for FDIS, ISO/IEC JTC 1/SC 27 N3757, unpublished 2003-11-30.
- ISO/IEC 17799: Code of Practice for Information Security Management. Document for FCD (2nd edition), ISO/IEC JTC 1/SC 27 N3948, unpublished 2004-06-17.
- ISO/IEC 13335-2: Information technology - Security techniques - Management of information and communications technology security (MICTS) - Part 2: Techniques for ICT security risk management. Text for 3rdWD, ISO/IEC JTC 1/SC 27 N3951, unpublished 2004-05-10.
- Supporting Document to ISMS requirements and preparatory documents "Information Security Management Systems - Specifications with Guidance for Use". ISO/IEC JTC 1/SC 27 N4036, unpublished 2004-06-26.
- BS 7799-2: Information Security Management Systems - Specifications with Guidance for Use. British Standard, London, 2002.
- ISO/IEC 13335: Information technology - Security techniques - Guidelines for the Management of IT security (GMITS). Technical Report, Genf, 2000.
- ISO/IEC 17799: Code of Practice for Information Security Management. International Standard, Genf, 2000.
- ISO/IEC 21827: Information technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM). International Standard, Genf, 2002.

www.decus.dePeter Berlich, Martina Rohde

IT Symposium 20052005-04-05

Normen der IT-Sicherheit im Vergleich Ende

Einleitung

Adress und Motivation

Begriffe und Ausgangssituation

Übersicht und Aufbau

Charakteristika von

Sicherheitsmanagementsystemen

Die Abstammungserkennung

Beurteilungskriterien

Anpassung an

Sicherheitsmanagement

Ausrichtung des

Sicherheitsmanagements

Ansatz im

Sicherheitsmanagement

Vergleich der Standards

ISO/IEC 17799: Code of Practice for Information Security Management

Beurteilung

ISO/IEC 13335: Management of information and communications technology security

Beurteilung

BS 7799-2: Information Security Management Systems - Specifications with Guidance for Use

Beurteilung

Zusammenfassung und Ausblick

Literaturverzeichnis

- Herzlichen Dank für Ihre Aufmerksamkeit!
- Fragen/Lob/Kritik/Anregungen?
- Kontakt:
 - peter.berlich@web.de
 - (peter.berlich@ch.ibm.com)
 - martina.rohde@cec.eu.int

www.decus.dePeter Berlich, Martina Rohde

IT Symposium 20052005-04-05