



SCIENTIFIC CONSULTING PARTNERS

S-ITsec: strategisches IT-Security-Managementsystem

IT-Sicherheit: Risiken erkennen, bewerten und vermeiden

„...Ein etabliertes IT-Security-Managementsystem (ISMS) ist ein kritischer Erfolgsfaktor für ein Unternehmen. Wichtig ist, die Sicherheit an den realen Bedrohungen auszurichten, um nicht „mit Kanonen auf Spatzen zu schießen...“

Gerhard Funk
Dipl.-Ing. TISP
Mitglied des SCOPAR-Beraterremiums



WISSEN - SCHAFFT - NUTZEN

Inhalt

	Seite
Internationale ISMS-Normen: die ISO 2700x-Familie	3
ISO 27001 – die „wesentlichen“ Kapitel	4
Arbeitspakete zur Etablierung eines ISMS	5
Reifegrade des ISMS	6
Bewertung von IT-Risiken	7
IT-Risikomanagement im ISMS	8
Mögliche Unterstützungsleistung von SCOPAR	9
Referenzen	10
Kontakt	11

Internationale ISMS-Normen: die ISO 2700x-Familie

Nummer	Titel	Status	Ursprung
ISO27000	Principles and vocabulary	in Entwicklung	Auf Basis von ISO13335 –1
ISO27001	ISMS Requirements	Veröffentlicht seit Oktober 2005	BS-7799:2 (außer Appendix B)
ISO27002	Code of Practice for ISMS	Ab 2007	ISO17799:2005
ISO27003	ISMS Implementation Guidance	in Entwicklung	Auf Basis von BS-7799:2 Appendix B
ISO27004	ISMS Metrics and Measurement	In Entwicklung, - Draft ist veröffentlicht	
ISO27005	ISMS Risk Management	in Entwicklung (Sept. 07 ?)	Auf Basis von ISO13335 –2

ISO 27001 – die „wesentlichen“ Kapitel

- Establishing the ISMS (4.2.1)
 - Define the scope and Boundaries of the ISMS; Define an ISMS policy; Define the risk assessment approach
 - Identify the risks; Analyze and evaluate the risks; Identify and evaluate options for the treatment of risks
 - Select control objectives for the treatment of risks
 - Prepare a Statement of Applicability
- Implement and operate the ISMS (4.2.2)
- Monitor and Review the ISMS (4.2.3)
- Maintain and Improve the ISMS (4.2.4)
- Documentation requirements – General (4.3.1); Control of documents (4.3.2); Control of records (4.3.3)
- Management commitment (5.1)
- Resource management (5.2)
- Internal ISMS audits (6.)
- Management review of the ISMS (7.)
- ISMS improvement (8.)

➤ **ISO 27001 gibt eine grobe Handlungsanleitung zur Einführung eines ISMS vor.**

Arbeitspakete zur Etablierung eines ISMS

- 1: Planung, Definitionen, Abgrenzungen, GAP-Analysen, Security Policy, Risikobehandlung, Maßnahmenplanung (**Phase PLAN**)
- 2: Umsetzung, Prozesse etablieren (Kommunikation, Dokumentation, Verantwortlichkeiten), Maßnahmenumsetzung (**Phase: DO**)
- 3: interne IT-Sicherheitsrevision durchführen, Status feststellen, Erfolgskontrolle (**Phase: CHECK**)
- 4: Optimierung des ISMS, Umsetzung von Korrekturmaßnahmen (**Phase: ACT**)
- 5: Ausdehnung des ISMS auf weitere Bereiche der IT, Übergang in Betriebsprozesse, Ende des Einführungsprojekts (**Phase: EXPAND**)

Das ISMS sollte keineswegs sofort mit der gesamten IT beginnen. Zu Beginn müssen die Aktivitäten auf einige wenige Schwerpunkte konzentriert werden. Das ISMS-Team muss die Arbeit mit den vielen kleinen IT-Sicherheitsprojekten in den unterschiedlichsten Reifegraden trainieren.

➤ **Auch bei ISMS gilt: Think big - start small!**

Reifegrade des ISMS

- 1: Es sind ad-hoc Ansätze für Prozesse und Verfahren im Einsatz.** Prozesse und Policies sind nicht definiert.
- 2: Ähnliche allgemeine Prozesse entwickeln sich, basieren aber auf Intuition und individueller Expertise.**
- 3: Verwendung von Good Practices entwickeln sich.** Prozesse, Policies und Verfahren sind für wesentliche Aktivitäten definiert und dokumentiert.
- 4: Die Prozesse sind rund und vollständig.** Interne Best Practices werden angewendet. Sämtliche Aspekte der Prozesse sind dokumentiert und wiederholbar. Policies wurden vom Management freigegeben. Standards zur Weiterentwicklung der Prozesse existieren und werden befolgt.
- 5: Externe Best Practices und Standards werden angewendet.** Die Prozessdokumentation wurde zu automatisierten Workflows entwickelt. Prozesse, Policies und Verfahren sind festgelegt und integriert und ermöglichen ein vollständiges, durchgängiges Management und Verbesserungen.

(Auszug aus dem CoBIT 4.0 Framework –
Attribute der Reife für Policies, Standards und Verfahren)

➤ **Je nach Sensibilität des Unternehmens oder -bereichs, sollte ein bestimmter Reifegrad erreicht sein.**

Bewertung von IT-Risiken

Es sind verschiedene Methoden anwendbar:

- Auf Basis der Schutzbedarfskategorien innerhalb der IT-Grundschutz-Vorgehensweise des BSI
- Nach SP800-30 des NIST. Das Ergebnis wird in einer übersichtlichen Risikomatrix dargestellt.
- Und weitere

Beispiel für eine Matrix zur Risikobestimmung:

		Wirkung				
		unbedeutend	gering	mittel	groß	katastrophal
Eintrittswahrscheinlichkeit	Fast sicher	mittel	bedeutend	hoch	hoch	hoch
	Wahrscheinlich	mittel	bedeutend	bedeutend	hoch	hoch
	Möglich	gering	mittel	bedeutend	hoch	hoch
	Selten	gering	mittel	mittel	bedeutend	hoch
	Sehr selten	gering	gering	mittel	bedeutend	bedeutend

➤ **Die konkreten Maßnahmen zu Erhöhung der Sicherheit müssen sich an der Wirkung einzelner Risiken orientieren.**

IT-Risikomanagement im ISMS

Eine detaillierte Risikoanalyse:

- Abgrenzung des Analysebereichs
- Identifikation der bedrohten Objekte
- Wertanalyse
- Bedrohungsanalyse
- Schwachstellenanalyse
- Identifikation bestehender Sicherheitsmaßnahmen
- Risikobewertung
- Auswertung

➤ **Die Anwendung der IT-Grundschutz-Vorgehensweise des BSI entspricht für den Schutzbedarf „normal“ der ISO 27001 und verkürzt den Prozess erheblich.**

Mögliche Unterstützungsleistung von SCOPAR

- **IT-Sicherheitsmanagement**

Unterstützung bei der Einführung eines anforderungsgerechten IT-Sicherheits-managements einschließlich aller dazu gehörenden Prozesse wie IT-Sicherheitsrevison mit internen Audits, IT-Risikomanagement und Dokumentenmanagement.

- **Interne Audits**

Interne Audits, die nicht zu einer Zertifizierung führen, können durchgeführt werden. Interne Audits (GAP-Analysen, Basis-Sicherheitschecks) sind wesentliche Tätigkeiten der internen IT-Sicherheitsrevison, die innerhalb des IT-Sicherheitsmanagements durchgeführt werden.

- **Risikomanagement**

Unterstützung beim Aufbau eines wirksamen Risikomanagement-Prozesses innerhalb des IT-Sicherheitsmanagements und bei der quantitativen und qualitativen Behandlung von Risiken.

- **Unterstützung, Coaching und Projektbegleitung**

Review und Anpassung vorhandener Dokumentationen

➤ **Die Experten von SCOPAR haben umfassende Erfahrungen in den unterschiedlichen Fragestellungen aus dem Bereich IT-Sicherheit.**

Referenzen (Auszug)

- Audit-Vorbereitung für ein Audit zum IT-Grundschutz-Zertifikat und zur Zertifizierung gemäß ISO 27001 auf Basis IT-Grundschutz bei einer Lebens- und Sachversicherung
- Entwicklung einer IT-Sicherheitsleitlinie für eine Großforschungseinrichtung
- Audit-Vorbereitung für ein Audit analog zu einem Audit zur Zertifizierung gemäß ISO 27001 auf Basis IT-Grundschutz für eine Behörde:
 - Vollständige Anwendung der IT-Grundschutz-Vorgehensweise
 - Strukturanalyse, Schutzbedarfsfeststellung, Modellierung, Basis- Sicherheitscheck, Ergänzende Sicherheitsanalyse, ergänzende Risikoanalyse
 - Erstellung von Richtlinien als Bindeglied zwischen der Sicherheitsleitlinie und den Feinkonzepten und als Arbeitsgrundlage für IT-Sicherheitsmanagement und IT-Revision

Wir freuen uns auf eine lange und erfolgreiche Zusammenarbeit!



SCIENTIFIC CONSULTING PARTNERS

SCOPAR - Scientific Consulting Partners
Maximilianstraße 35a
D - 80539 München

Fon: +49 - 89 - 958 98 065
Fax: +49 - 89 - 958 98 066
E-Mail: info@scopar.de

WISSEN - SCHAFFT - NUTZEN