ISMS für KMU

Wirksames Informationssicherheitsmanagement nach ISO 27001

Informationssicherheitsmanagementsystem (ISMS) für kleine und mittlere Unternehmen: Eine Zusammenfassung einer Projektstudie am Kompetenzzentrum für Sicherheits- und Risikomanagement der ZHAW Winterthur

Wieso ermöglicht ein ISMS ein nachweislicher und wirksamer Umgang mit Geschäftsrisiken?

Welche sowieso zu lösenden Herausforderungen können mit einem „ISMS für KMU“ ebenfalls gelöst werden?

Von Christoph Koch.

Was ist ein ISMS? Wieso soll ein KMU ein ISMS bauen?

Unter einem ISMS wird ein Vorgehen in Organisationen oder Unternehmen jeder Grösse, Branche und Komplexität verstanden, welche Geschäftsrisiken bezüglich Information angemessen und auf die jeweilige Organisation angepasst bewirtschaften wollen. Informationen stellen in jeder Organisation das Rückgrat und den Lebensnerv dar. Hier ein Beispiel zur Wichtigkeit und Bedeutung von Informationen: Ein Produktionsunternehmen muss Informationen zu den hergestellten Produkten angemessen schützen. Andernfalls kann im Schadenfall beispielsweise weder produziert, noch an Kunden ausgeliefert werden.

Damit ein solcher Schadenfall ***nicht*** geschehen kann:

- ✓ Müssen Informationen korrekt (nicht verfälscht), vertraulich (der Konkurrenz unbekannt) und über den ganzen Prozess verfügbar (keine Ausfälle während der Produktionszeit) sein.
- ✓ Diese Anforderung betrifft vorrangig die kritischen Abläufe (Teilprozesse, Prozesse in der Organisation)

Es stellt sich die Frage, ob diese kritischen Abläufe in KMU einerseits:

- ✓ bekannt sind
- ✓ und andererseits angemessen mit Gegenmassnahmen optimiert werden.

Ein ISMS adressiert diesen Sachverhalt und stellt die regelmässige Anpassung auf ändernde Situationen in der Organisation sicher.

Was bedeutet ISO 27001?

Die Norm ISO/IEC 27001:2005 fasst die **Anforderungen** an ein Informationssicherheitsmanagementsystem zusammen. Diese Norm kann vergleichbar mit der Norm ISO 9001 weltweit zertifiziert werden:

- ✓ In der Schweiz können beispielsweise die Unternehmen SQS, SGS und KPMG ein ISMS nach ISO 27001 zertifizieren.
- ✓ Gemäss der Schweizerischen Akkreditierungsstelle sind in der Schweiz circa 22 Unternehmen nach ISO 27001 zertifiziert. Stand Q1/2010, siehe SAS [2010].
- ✓ Ein ISMS bringt dem Unternehmen ein vergleichbares Sicherheitslevel (Benchmark), welches Vertrauen zu Kunden, Lieferanten oder anderen Anspruchsgruppen schaffen kann.

Motivation und Ziele der Projektstudie

Die Projektstudie geht von den folgenden Annahmen aus:

- ✓ Ein KMU hat keine, bzw. zu wenig Ressourcen für den Design, die Planung und Umsetzung eines organisationsspezifischen ISMS.
- ✓ Ein KMU verfügt nicht, bzw. über zu wenig Wissen und Erfahrung für die Aufgabe, ein ISMS-Projekt erfolgreich umsetzen zu können.

Aus diesen Thesen wurden die Ziele abgeleitet:

- ✓ Identifikation der ISMS-Regelungsbereiche
- ✓ Identifikation der Komponenten eines ISMS
- ✓ Verwendungen bekannter Hilfsmittel aus den Bereichen Capability/Maturity Modellen (CMMI, ISM3, RiskIT) und Risikoanalysemethoden
- ✓ Erstellung eines ISMS-Leitfadens abgestützt auf ISMS-Komponenten und bekannten, oben erwähnten Hilfsmitteln
- ✓ Abgrenzung der Bedeutung des entwickelten ISMS-Leitfadens, bzw. der ISMS-Lösung

Klassifizierung von KMU

Als Alternative zu der Klassifizierung von Organisationen gemäss ISO 27006, [2007, Seite 19]

wurde die Klassifizierungsweise gemäss Tabelle 1 verwendet.

Tab. 1: Klassifizierung von KMU

Klassifizierung	Mgmt System	Prozessdoku	OR728a/IKS	Fortg. Modelle S/E/E
1	N	N	N	N
2a	J	N	N	N
2b	N	J	N	N
2c	N	N	J	N
3a	J	J	N	N
3b	N	J	J	N
3c	J	N	J	N
4	J	J	J	N
5	J	J	J	J

Quelle: © 2010 Christoph Koch, Winterthur

Erklärung zur Tabelle 1:

Mgmt System:
Ein Ja (J) bedeutet, dass die Organisation mindestens ein Management System geplant, umgesetzt oder in der Umsetzungsphase hat. Beispiele: ISO 9001/ QMS; ISO 14001/ EMS.

Prozessdoku:
Ein Ja (J) bedeutet, dass die Organisation zumindest die bedeutenden Prozesse im Unternehmen dokumentiert hat. Bedeutende Prozesse sind zum Beispiel: Kernprozesse, Geschäftsprozesse, die den Hauptumsatz/ Hauptgewinn eines Unternehmens ausmachen.

OR 728a/IKS:
Ein Ja (J) bedeutet, dass die Organisation verpflichtet ist, gemäss Schweizer Obligationenrecht eine ordentliche Revision durchführen zu lassen und daher der Nachweis eines IKS von der buch- und rechnungslegungsprüfenden Organisation gefordert wird.

Fortg. Modelle S/E/E:
Ein Ja (J) bedeutet, dass die Organisation fortgeschrittene Modelle zu Sicherheit, Effizienz und Effektivität (fortg. Modelle S/E/E) verwendet. Beispiele solcher Modelle sind: ISO 27001, CMMI, Six Sigma, ITIL/ ISO 20000, ISO 31000 oder andere. Entscheidend dabei ist, dass mehrere Risiko-/ Chancen-Kriterien in ein umfassendes, ganzheitliches Management System integriert sind.

Folgende weitere Kriterien zur Tabelle 1 können zusätzlich in die Klassifikation einfliessen:

- ✓ Organisationen, die Sicherheitsrollen bzw. sicherheitsverantwortliche Personen ohne zusätzliche Fachverantwortung einsetzen, Beispiele: Sicherheitsbeauftragter, Sicherheitsverantwortlicher, Chief Information Security Officer CISO, Chief Security Officer (CSO). Funktionen bzw. Personen wie Qualitätsverantwortlicher, Umweltbeauftragter können ebenfalls einfliessen.
- ✓ Organisationen, die organisationsübergreifend eine Projektmanagement-Methodik erfolgreich einsetzen. Beispiele: Systems Engineering gemäss Haberfellner et al [2002], PMBOK, Prince II oder andere.
- ✓ Organisationen, die Führungsmodelle, bzw. –Methoden erfolgreich einsetzen (z. B. Kairies [2007], Müller [2005]).

These zu KMU-Anforderungen
Der Autor stellt die nachfolgende These zu den Anforderungen von KMU auf:

- ✓ **Das Verhältnis von Kosten/ Nutzen des ISMS muss ausgewogen sein**: Es sollen so viel Ressourcen in ein ISMS investiert werden, wie für die Zielerreichung der spezifischen, angestrebten KMU-Ziele notwendig sind. Ein zertifizierbares ISMS muss nicht vorrangig zu den notwendigen KMU-Zielen gehören. Ein nicht-zertifizierbares ISMS in der Ausprägung „Basis-ISMS für KMU“ kann KMU-Ziele durchaus erfüllen.
- ✓ **Einfaches & klares ISMS**: Ein einfaches ISMS ist in der Praxis besser umsetzbar, involvierte Personen und Personengruppen sind in der Lage, das ISMS zu verstehen. Der grösste Nutzen eines Management Systems wird dadurch erreicht, wenn die dazugehörigen Aktivitäten und Vorgehensweisen, z. B. „Code of Practices[1]“ regelmässig in einer definierten Umsetzungsqualität ausgeführt werden. Ein wichtiger Aspekt bezüglich der Umsetzungsqualität stellt das aktuelle Sicherheitsbewusstsein der Mitarbeiter dar. Zur Wahrung eines definierten Sicherheitslevels muss das Sicherheitsbewusstsein regelmässig geprüft und gegebenenfalls mit Massnahmen zu Gunsten der ISMS-Ziele optimiert werden.

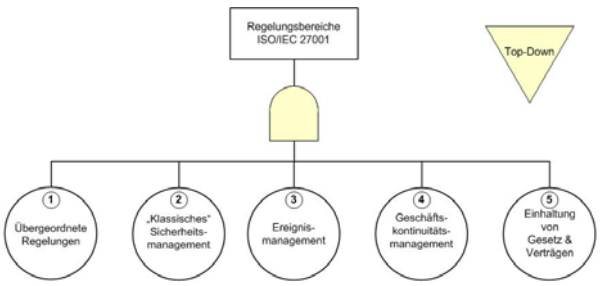
[1] [ISO 27002:2007]. Der „Code of Practice“ beschreibt Massnahmen, die ein ISMS gemäss [ISO27001:2005] ermöglichen. These des Autors: Für ein „ISMS für KMU“ können wesentlich weniger Massnahmen ausreichen.

- ✓ **Umsetzbares & praxisnahes ISMS**: Das ISMS muss in der jeweiligen Organisation umsetzbar sein. Mit anderen Worten: Das konzipierte Management System (ISMS) muss in die bestehende Organisation eingebettet werden können. Je nach Stand der jeweiligen Organisation bedeutet die Einbettung eines ISMS die Integration in die Prozesse bzw. in das angewendete Prozessmodell der betreffenden Organisation. Das ISMS ist zumindest in die Kernprozesse der Organisation einzubetten.
- ✓ **Nicht-Experten können das ISMS, bzw. die damit zusammenhängenden Aktivitäten in der täglichen Arbeit anwenden**: Ein Erfolgskriterium für ein nachhaltiges ISMS ist deren konsequente, permanente Anwendung durch alle Personen in der Organisation. Jede Person in der Organisation trägt dazu seinen Teil zum Gesamterfolg, auch zum Misserfolg, bei.

Vorgehen zur Entwicklung eines unternehmensspezifischen ISMS
Die ISMS-Entwicklung stützt sich auf die fünf Regelungsbereiche von ISO 27001 ab, siehe Abb. 2:

1. Übergeordnete Regelungen
2. Sicherheitsmanagement
3. Ereignismanagement
4. Geschäftskontinuitätsmanagement
5. Einhaltung von Gesetzen, vertraglichen und branchenspezifischen Verpflichtungen.

Abb. 2: Top-Down-Vorgehen & Regelungsbereiche ISO 27001

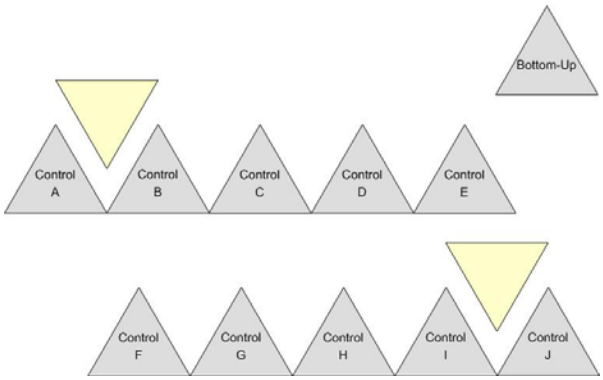


Quelle: © 2010 Christoph Koch, Winterthur

Dabei werden bekannte Aspekte aus Risikoanalysemethoden angewendet, beispielsweise das Top-Down- und das Bottom-Up-Vorgehen. Je nach Anforderungen können weitere Aspekte, beispielsweise aus den Modellen CMMI, ISM3 und RiskIT in die ISMS-Entwicklung einfliessen.

Die Abbildung 3 zeigt schematisch das passende Bottom-Up-Vorgehen zum erwähnten Top-Down-Vorgehen gemäss Abbildung 2 auf:

Abb. 3: Bottom-Up-Vorgehen ISO 27001



Quelle: © 2010 Christoph Koch, Winterthur

ISMS für KMU nach ISO 27001
Die hier aufgeführten Aspekte zeigen den Rahmen eines „ISMS für KMU" auf:

- ✓ **Gewaltentrennung/ Rollenteilung**: Der Entscheidungsträger bezüglich Informationssicherheit sollte nicht gleichzeitig für eine Fachfunktion und die Informationssicherheit verantwortlich sein.
- ✓ **ISMS Policy**: Anstelle einer ISMS Policy soll eine **ISMS-Leitlinie** und eine **Informationssicherheitsleitlinie** erstellt werden.
- ✓ **ISMS-Leitlinie**: In der ISMS-Leitlinie werden die Rahmenbedingungen und die für die Umsetzung notwendigen Komponenten für ein ISMS festgehalten. Verantwortliche Stellen: Alle Personen, welche für das Management des betreffenden ISMS verantwortlich sind.
- ✓ **Informationssicherheits-Leitlinie**: In der Informationssicherheits-Leitlinie wird Informationssicherheit für alle Personen und Bereiche einer Organisation verbindlich und verständlich beschrieben. Verantwortliche Stellen: Alle Mitarbeitenden im Zielbereich bzw. in der betreffenden Organisation.
- ✓ **Inventar** (Inventory of Information Assets): Das Inventar enthält alle bedeutenden und wichtigen Informationswerte bzw. Schutzobjekte im Zielbereich.
- ✓ **Notwendige Dokumente** (Mandatory Documents): Alle vorgeschriebenen Dokumente für den Zielebereich sind zu erstellen. Ein „ISMS für KMU" enthält zumindest diese Dokumente:
  - o ISMS Policy gemäss oben mit den beiden Dokumenten bzw. Kapiteln „**Informationssicherheits-Leitlinie**" und „**ISMS-Leitlinie**"

- o **Erklärung zur Anwendbarkeit in der Organisation** (Statement of Applicability SoA) welche zu allen Massnahmen (Controls) klärt, ob diese in der betreffenden Organisation, bzw. im Zielbereich anwendbar (applicable) oder nicht anwendbar (not applicable) sind. Beide Fälle müssen schriftlich begründet werden.
- o **Risk Treatment Plan (RTP)** zeigt auf, wie die Organisation wesentliche, bzw. bedeutende Risiken mit dem ISMS organisationsspezifisch und angemessen bewirtschaftet.
- o Je nach Zielsetzung und angestrebtem Reifegrad (Maturitätsstufe) können weitere Dokumente notwendig werden.

✓ Beschreibung der kontext-, bzw. organisationsspezifischen Grundsätze (Policy gemäss oben), des **Frameworks (PDCA Cycle)** und des **Risikomanagements** in einer angemessenen Detaillierungstiefe.

Reifegrad 0 entspricht „Basis-ISMS für KMU"
Das Resultat der Studie zur Idee „ISMS für KMU" lässt sich gemäss Tabelle 2 zusammenfassen.

Tab. 2: Reifegrad Stufe 0 „Basis-ISMS für KMU"

Level	*Erklärung*
Level 0: Basis-ISMS für KMU[71]	Dieser Level repräsentiert ein sehr schlankes ISMS, welches dem implementierenden Unternehmen Nutzen generiert. Das ISMS mit der Reifegradstufe 0 besteht aus sieben Komponenten: Zielsetzungen zum ISMS-Kontext, Sicherheitsrollen, ISMS Policy, Inventar der Schutzobjekte, Erklärung zur Anwendbarkeit in der Organisation (SoA) bzw. notwendige Dokumente, Risikomanagement mittels ISMS, Fortschritts- und Erfolgskontrolle (PDCA-Prozess).

Quelle: © 2010 Christoph Koch, Winterthur

Die Reifegradstufe 0 beschreibt ein ISMS mit „sehr tiefem Reifegrad". Ein solches ISMS kann gerade noch als ISMS bezeichnet werden. Man spricht auch von einem „kleinstmöglichen" oder von einem „**Basis-ISMS**".

Fazit der Studie*
Mit dem Leitfaden der Studie sind auch kleine und mittlere Unternehmen (KMU) und Organisationen in der Lage, mit einem chancen-risikobasierenden Modell die Geschäftsziele mit dem Fokus auf Informationssicherheit zu unterstützen, beziehungsweise sicherzustellen.
Weiter können je nach spezifischer Zielsetzung Anforderungen eines internen Kontrollsystem IKS und einer Geschäftskontinuitätsplanung durch ein ISMS gelöst werden.
Zudem sind Organisationen mit einer derart integrierten Lösung in der Lage, bei Bedarf weitere Schitte bis zum Ziel eines integrierten Risikomanagementsystems IRM im Sinne von ISO 31000 auszuführen.

Autor des Artikels und der Projektstudie

Christoph Koch,
Inhaber & Gründer von Koch IS GmbH,
Spezialisten für Informationssicherheit und angewandtes Risikomanagement,
Winterthur.

*Am 25. Mai 2010 findet ein Anlass bei ISACA Schweiz statt. An diesem Anlass wird die Studie erklärt. Weitere Informationen unter www.isaca.ch unter „After Hour Session" und unter www.koch-is.ch, „Neuigkeiten" zu finden.

Quellennachweise:
Studie "Basis-ISMS konform zu ISO//IEC 27001 für kleine und mittlere Unternehmen":
Koch, Christoph (2010), Winterthur. Unveröffentlichte Studie am Kompetenzzentrum für Sicherheits- und Risikomanagement (KSR), Zürcher Hochschule für angewandte Wissenschaften in Winterthur (ZHAW). Hinweis: Das Management Summary und Inhaltsverzeichnis sind öffentlich zugänglich. Siehe www.koch-is.ch unter „Neuigkeiten".

CMMI:
[CMMI-ACQ 2007] CMMI Product Team (2008): Improving processes for acquiring better products and services. CMMI® for Acquisition, Version 1.2, November 2007. Carnegie Mellon University. Unlimited distribution subject to the copyright.
[CMMI-UND 2007] CMMI Product Team (2007): Understanding and Leveraging a Supplier's CMMI® Efforts: A Guidebook for Acquirers. March 2007. Carnegie Mellon University. Unlimited distribution subject to the copyright.

Haberfellner:
Haberfellner, Nagel, Becker, Büchel, von Massow (2002): Systems Engineering. Methoden und Praxis. 11. Auflage.Hrsg.: W. F Daenzer, F. Huber. Zürich: Verlag Industrielle Organisation.

ISM3:
Information Security Management Maturity Model ISM3 (2009): Information Security Management Maturity Model, ISM3. V2.1 ist kostenlos verfügbar via http://www.ism3.org. Aktuelle Version: V2.3. via URL: www.lulu.com/content/paperback_book/information_security_management_maturity_model_v23/6441763 [Stand: 1. Oktober 2009].

ISO 27001:
International Organization for Standardization, International Electrotechnical Commission (2005): ISO/IEC 27001:2005 Information Technology — Security Techniques — Information Security Management Systems — Requirements. Geneva.

ISO 27002:
International Organization for Standardization, International Electrotechnical Commission (2007): ISO/IEC 27002:2007 (=ISO/IEC 17799:2005). Security Techniques — Code of Practice for
Information Security Management. Geneva.

ISO 27006:
International Organization for Standardization, International Electrotechnical Commission (2007): ISO/IEC 27006:2007 Information Technology — Security Techniques — Requirements for Bodies providing Audit and Certification of Information Security Management Systems. Geneva.

ISO 31000:
International Organization for Standardization (2009): ISO 31000. Risk management - Principles and guidelines. It provides principles and generic guidelines on risk management. Geneva.

ISO Guide 73:
ISO/IEC Guide 73:2002, Risk management Vocabulary. Guidelines for use in standards.

Kairies:
Kairies, Peter (2007): Moderne Führungsmethoden für Projektleiter. Professionelles Projektmanagement – Erfolgsfaktoren –Praxistipps. 2. Auflage. Renningen (D): Expert Verlag.

Müller:
Müller, Klaus-Rainer (2005): Handbuch Unternehmenssicherheit. 1. Auflage. TQU Steinbeis- Transferzentren Qualität im Unternehmen.

RiskIT:
ISACA (2009): The Risk IT Framework. Based on CobIT and Val IT. A member confidential publication of ISACA. Rolling Meadows: ISACA. URL:
http://www.isaca.org/Template.cfm?Section=Risk_IT&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=79&ContentID=48749 [Stand: 1.Februar 2010]

SAS 2010:
Schweizerische Akkreditierungsstelle (2009): Staatssekretariat für Wirtschaft SECO. Informationssicherheit. ISMS. URL: http://www.seco.admin.ch/sas/00229/00239/index.html?lang=de [Stand: 1. Februar 2010]

Zu den Leistungen von Koch IS GmbH gehören:

- ✓ Unterstützung in den Regelungsbereichen von Informationssicherheit/ ISO 27001
- ✓ Durchführen von Risiko- und Auswirkungsanalysen (Risk Analysis, Business Impact Analysis)
- ✓ Entwicklung von Business Continuity Strategien im Umfeld des Business Continuity Managements
- ✓ Analyse der Ist-Situation, Design und Umsetzungsbegleitung im Umfeld von internen Kontrollsystemen IKS
- ✓ Unterstützung in den Regelungsbereichen von „angewandtem Risikomanagement“ gemäss ISO 31000.