Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

IMB Institute of Management Berlin

# Das GQMS-Vorgehens-modell für das Messen der Wirksamkeit von Informationssicherheits-managementsystemen

Authors: Rainer Rumpel
Editors: Carsten Baumgarth | Gert Bruche | Christoph Dörrenbächer | Friedrich Nagel

Working Paper No. 83
06/2015
Series Editor: Head of IMB Institute of Management Berlin

CONCEPTUAL PAPER

# Das GQMS-Vorgehensmodell für das Messen der Wirksamkeit von Informationssicherheitsmanagementsystemen

**Rainer Rumpel**

Paper No. 83, Date: 06/2015

Working Papers of the
Institute of Management Berlin at the
Berlin School of Economics and Law (HWR Berlin)
Badensche Str. 50-51, D-10825 Berlin

Editors:
Carsten Baumgarth
Gert Bruche
Christoph Dörrenbächer
Friedrich Nagel

ISSN 1869-8115

## Biographic Note:

Prof. Dr. **Rainer Rumpel** ist Professor für Allgemeine Betriebswirtschaftslehre, insbesondere Wirtschaftsinformatik am Fachbereich Duales Studium der Hochschule für Wirtschaft und Recht Berlin. Er erhielt von der Humboldt-Universität zu Berlin den Grad Doktor der Naturwissenschaften. Schwerpunkt seiner Lehrtätigkeiten sind IT-Infrastrukturen. Er forscht hauptsächlich auf dem Gebiet des Informationssicherheitsmanagements. Er prüft Unternehmen auf ihre Konformität mit der internationalen Norm ISO/IEC 27001 (Anforderungen an Informationssicherheitsmanagementsysteme). Er war mehrere Jahre lang als IT-Berater bei einem führenden deutschen Systemhaus tätig.

Prof. Dr. **Rainer Rumpel** is a professor of Information Systems Engineering at the Berlin School of Economics and Law. He holds a doctoral degree in science from Humboldt Universität Berlin. His emphasis of lecturing is on IT infrastructures. His main research interest is related to Information Security Management. He is auditing enterprises to check conformity with the international standard ISO/IEC 27001 (Information Security Management Systems Requirements). Several years he was acting as IT consultant at a leading German system vendor.

METROSEC

**Forschungsprojekt zur Messung, Analyse und Bewertung von Managementsystemen für Informationssicherheit**

Es haben mitgewirkt:

**Rolf-Dieter Kasper**, RWE Deutschland AG

**Peter Thanisch**, RWE Deutschland AG

**Lucas Pentzek**, Hochschule für Wirtschaft und Recht Berlin

Mit freundlicher Unterstützung von:

VORWEG GEHEN

## Abstract:

The meaning of a management system is to establish systematic and continuous reliable procedures. Potential for improvement should be identified to realize improvement and to achieve evidence for them. Meanwhile, many organizations operate management systems. In Europe, around 8,000 companies run a certified information security management system. Several companies struggle with the requirement to evaluate the effectiveness of the system plausible and traceable.

In this elaboration a process model is presented which offers a rigorous approach for evaluating the effectiveness of the management system and the performance of information security. Process approach, goal question metric and strict adjustment to the standard ISO/IEC 27001 have been important success factors for the planning of the method.

## Zusammenfassung:

Der Sinn eines Managementsystems besteht darin, Abläufe systematisch und gleichbleibend verlässlich zu gestalten. Es sollen Verbesserungspotentiale erschlossen werden, um Verbesserungen vorzunehmen und nachweisbar zu erreichen. Viele Organisationen betreiben mittlerweile Managementsysteme. In Europa haben ca. 8.000 Unternehmen ein zertifiziertes Informationssicherheitsmanagementsystem in Betrieb. Viele Unternehmen haben das Problem, die Effektivität des Systems plausibel und nachvollziehbar bewerten zu können.

In dieser Ausarbeitung wird ein Vorgehensmodell präsentiert, das mit der gebotenen Einfachheit und der notwendigen Fundierung ein stringentes Verfahren zur Bewertung der Wirksamkeit des Managementsystems und der Informationssicherheitsleistung bietet. Wesentliche Erfolgsfaktoren bei der Konzeptionierung des Verfahrens waren die Prozessorientierung, der Goal-Question-Metric-Ansatz und die konsequente Ausrichtung an der Norm ISO/IEC 27001.

## Inhalt

## Einleitung

***„Miss alles, was sich messen lässt, und mach alles messbar, was sich nicht messen lässt.“***

Archimedes

Managementsysteme sind heutzutage anerkannte Werkzeuge der Unternehmensführung. Mehr als 56.000 Unternehmen in Deutschland sind gemäß ISO 9001 zertifiziert.[1] Wenn man von der Statistik der ISO zu Konformitätszertifikaten ausgeht [2], so sind die in Unternehmen am häufigsten betriebenen Managementsysteme:

- Qualitätsmanagementsystem (gemäß ISO 9001)
- Umweltmanagementsystem (gemäß ISO 14001)

Die internationale Norm ISO 9001 stellt diverse Anforderungen an ein Qualitätsmanagementsystem. Unter anderem wird von zertifizierten Unternehmen gefordert, dass sie Messprozesse realisieren, die dazu beitragen, die Wirksamkeit des Qualitätsmanagementsystems zu verbessern.[3]
Mittlerweile gibt es in Europa knapp 8.000 Unternehmen, die gemäß ISO/IEC 27001 zertifiziert sind, die also ein zertifiziertes Informationssicherheitsmanagementsystem (ISMS) besitzen. In dieser Norm wird verlangt, dass die Wirksamkeit des ISMS und die Leistung der Informationssicherheit bewertet werden. Zu diesem Zweck müssen Messmethoden festgelegt werden.[4]
Ist das Zitat von Archimedes[5] berechtigt? Was ist der Sinn des Messens? Messen ist Vergleichen.[6] Ich vergleiche beispielsweise die Länge eines Stabes mit der Anzahl gleich langer Einheitslängen (Zollstock). Aber man muss nicht immer quantitativ vergleichen. Man kann auch qualitativ vergleichen. Beispielsweise kann man zwei Stäbe nebeneinander stellen und deren Länge vergleichen, ohne quantitative Messwerte zu erheben. Man kann anhand einer Ordinalskala auch mehrere Stäbe miteinander vergleichen (längster, zweitlängster, drittlängster usw.). Bei Stablängen ist diese Art des qualitativen Vergleichs relativ leicht durchzuführen. Aber wie ist das bei Managementsystemen? Wie kann man herausfinden, welches das effektivere von zwei ISMS ist oder ob das vorhandene ISMS letztes Jahr effektiver war als vorletztes Jahr?

***Effektivität* ist ein Maß für die Zielerreichung und kann als Synonym von *Wirksamkeit* angesehen werden.**

Wenn ein quantitativer Vergleich möglich ist, dann gibt es eine Messgröße für die Effektivität *Eff* und man kann ermitteln, ob

$$Eff(ISMS1) > Eff(ISMS2)$$

ist. *Eff* ist ein sogenannter Schlüsselindikator für die Wirksamkeit des ISMS.

Die Beantwortung der folgenden Fragen ist das zentrale Ziel der vorliegenden Ausarbeitung:

1. Ist es möglich einen quantitativen Effektivitätsindikator für ISMS systemunabhängig herzuleiten?
2. Ist das zugehörige Vorgehensmodell eine solide und verständliche theoretische Grundlage für das Messen, Analysieren und Bewerten der Effektivität von ISMS, dessen Anwendbarkeit und Verständlichkeit ausreichend ist, um beträchtliche Akzeptanz bei den Zielgruppen zu erreichen?

[1] Siehe http://www.iso.org/iso/iso-survey
[2] Siehe http://www.iso.org/iso/iso-survey
[3] [ISO9001], S. 43
[4] [ISO27001], S. 7
[5] Einige Quellen führen diese Aussage auf Galileo Galilei zurück.
[6] In etlichen Fällen ist Zählen eine Alternative zum Messen.

Um die Schwierigkeit gültigen Messens zu veranschaulichen, nehmen wir das Beispiel eines elektrischen Stromkreises. Man kann die Stromstärke messen, indem man die Helligkeit (Lichtstrom) der Lampe misst (siehe Abbildung 1). Aber diese Messung ist nicht verallgemeinerbar, wenn es nicht strenge Vorgaben hinsichtlich der Materialeigenschaften der Lampe gibt. Verwendet ein anderer die primitive Messregel „Miss die Stromstärke, indem Du die Helligkeit der Lampe misst“ umsetzt, dann kann ein anderer Stromkreis eine hellere Lampe aufweisen, obwohl die Stromstärke geringer ist, wenn beispielsweise eine Halogenlampe statt einer Glühlampe im Einsatz ist. Weiterhin könnte eine andere Spannungsquelle mit höherer Spannung im Einsatz sein. Schließlich kommt erschwerend hinzu, dass der Zusammenhang zwischen Lichtstrom und elektrischer Stromstärke nichtlinear ist.

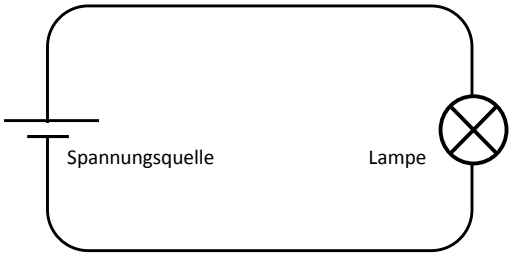


*Abbildung 1: Stromkreis*

Es ist also evident, dass zum Vergleich von Systemen eine möglichst präzise Messmethode erforderlich ist, die Vergleichbarkeit ermöglicht und Messgrößen zum Einsatz kommen, die relevant für die zu messende Größe sind. Der Umsetzbarkeit dieser Anforderungen soll im Folgenden für ISMS nachgespürt werden.
Wenn es möglich sein sollte, die Wirksamkeit eines ISMS bzw. die Leistung der Informationssicherheit robust zu messen, dann kann man den Istzustand angemessen bewerten und Verbesserungen bzw. Verschlechterungen zuverlässig feststellen.
Nach der Vorstellung wichtiger Grundbegriffe werden zunächst die Anforderungen dargestellt, die an Informationssicherheitsmanagementsysteme hinsichtlich der Wirksamkeitsbewertung gestellt werden. Anschließend wird vermittelt, welche Faktoren bzw. Methoden bei der Anbahnung der Wirksamkeitsermittlung erfolgversprechend sind. Im Mittelpunkt der Ausarbeitung steht die Vorstellung eines Verfahrens zur Bewertung der Effektivität der Management- und Informationssicherheitsprozesse.

Die Fallbeispiele stammen aus dem Bereich der intelligenten Stromnetze (Smart Grid).

# 1 Begriffliche Grundlagen

## Prozesse

***“Security is a business process. If you are not measuring and controlling the process, you are not measuring and controlling security.”***
Lance Hayden

Viele Unternehmen sind aufgrund der Komplexität des Tätigkeitsfelds bzw. der Unternehmensstruktur darauf angewiesen, die Arbeitsabläufe strikt zu organisieren und zu dokumentieren. Es sind also Prozesse zu verwalten.


*Abbildung 2: Aufbau eines einfachen Prozesses*

Ein Prozess ist ein "Satz von in Wechselbeziehungen oder Wechselwirkung stehenden Tätigkeiten, der Eingaben in Ergebnisse umwandelt."[7] Wesentlich für einen Prozess ist neben dem Tätigkeitsmuster also das Vorhandensein eines Inputs und eines Outputs. Ein typisches Beispiel ist der Softwareentwicklungsprozess.

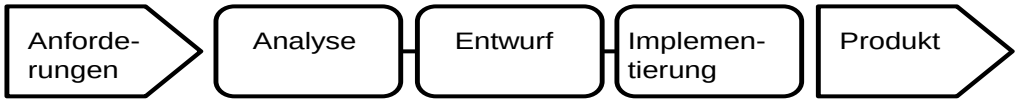


*Abbildung 3: Softwareentwicklungsprozess (vereinfacht)*

Ein Geschäftsprozess ist ein Prozess, der wertschöpfende Aktivitäten derart miteinander verknüpft, dass die von Kunden erwarteten Leistungen erbracht werden.[8] Einen Prozess, der einen oder mehrere Geschäftsprozesse unterstützt, aber keine eigene Wertschöpfung erzielt, nennt man „Unterstützungsprozess". IT-Prozesse sind in der Regel Unterstützungsprozesse. Unterstützungsprozesse wie zum Beispiel IT-Prozesse haben bei der Unterstützung von Geschäftsprozessen heutzutage solch eine grundlegende Bedeutung, dass der Wert der Unterstützung nicht unterschätzt werden sollte. Wichtige Elemente eines Prozesses sind: Bearbeitungsobjekt, Ressourcen, Eingaben, Ergebnisse, besondere Prozessanforderungen.

## Managementsysteme

Ein Managementsystem ist ein Satz zusammenhängender und sich gegenseitig beeinflussender Elemente einer Organisation, um Ziele, Richtlinien und Prozesse zum Erreichen dieser Ziele festzulegen.[9] Es ist augenfällig, dass ein offenes System, ein System mit Ein- und Ausgang, Ähnlichkeit mit einem Prozess besitzt.

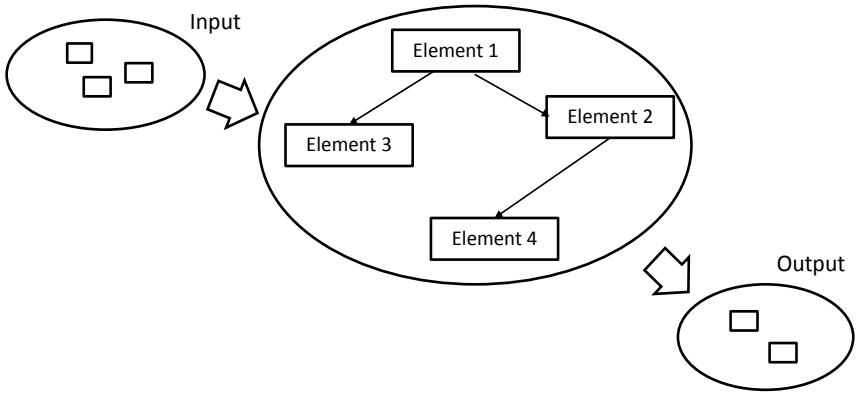


*Abbildung 4: Offenes System*

Gemäß der Struktur des gemeinsamen Textes von ISO/IEC für Managementsysteme sind zentrale Elemente eines Managementsystems: Führung, Planung, Unterstützung, Betrieb, Bewertung, Verbesserung.[10] Man kann also ein Managementsystem als ein **System von Managementprozessen** auffassen.

## Informationssicherheitsmanagementsystem (ISMS)

Ein Informationssicherheitsmanagementsystem (ISMS) umfasst Politik, Verfahren, Richtlinien und damit verbundene Ressourcen und Tätigkeiten, die von einer Organisation gelenkt werden, um ihre

[7] [ISO9000], S.20
[8] [SSE2013], S.53
[9] [ISO27000], S.16
[10] Vgl. [ISO2013], S.141-146 (Annex SL)

Informationswerte zu schützen. Ein ISMS ist ein systematisches Modell für die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Pflege und die Verbesserung der Informationssicherheit der Organisation, um Unternehmensziele zu erreichen.[11]

## 2 Anwendungshintergrund: Smart Grid

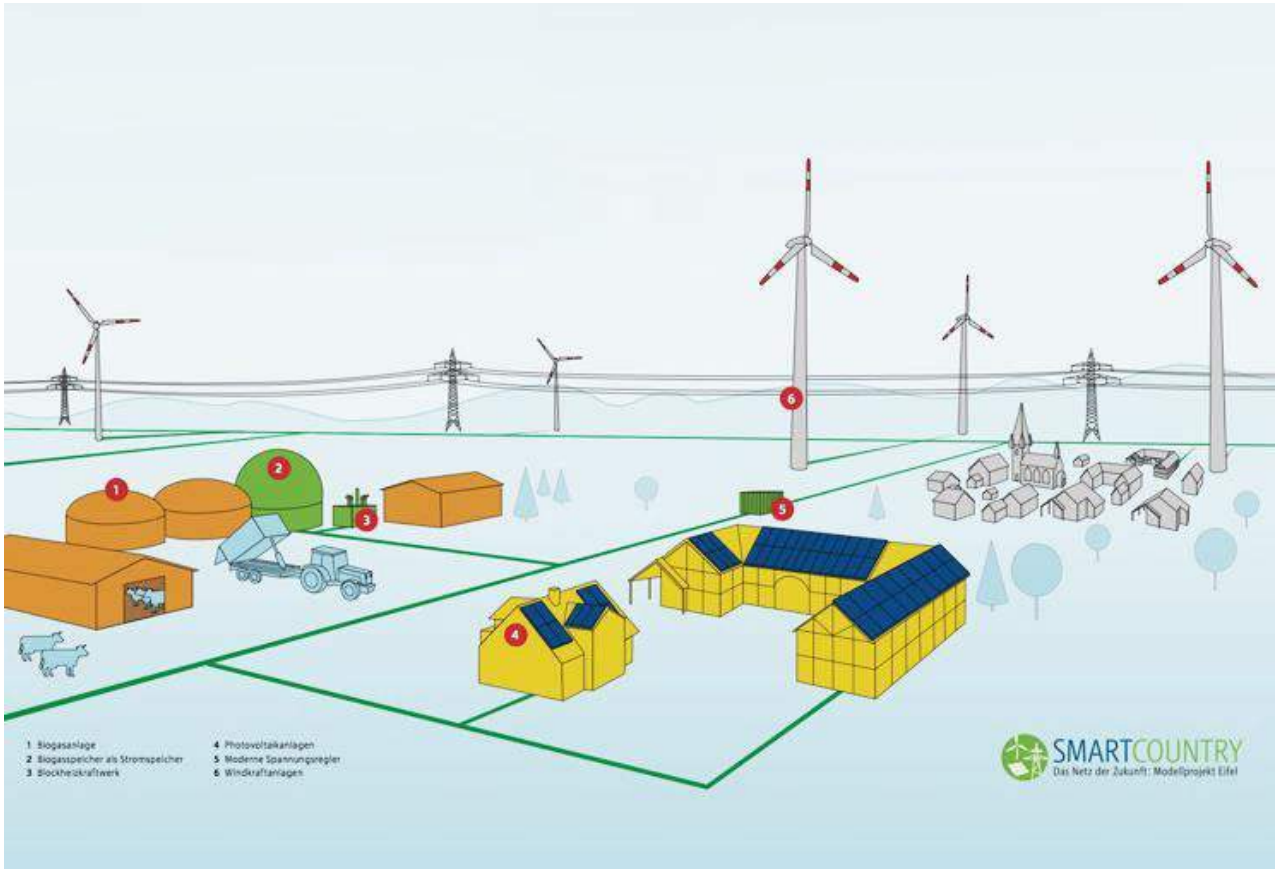


*Abbildung 5: Dezentrale Energieverteilung (Quelle: RWE)*

Energienetze gehören zu den sogenannten kritischen Infrastrukturen. Das Bundesamt für Sicherheit in der Informationstechnik definiert wie folgt: „Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“[12] Als kritische Infrastruktur sind Energienetzbetreiber dem Energiewirtschaftsgesetz unterworfen, das die Betreiber in §11 unter anderem dazu verpflichtet „einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die der Netzsteuerung dienen, zu gewährleisten“. Die Bundesregierung plant zusätzlich die Einführung eines ergänzenden Sicherheitskatalogs, in dem nach dem derzeitigen Wissensstand gefordert wird, dass die Energienetzbetreiber ein ISMS einführen.

### Verteilnetze

Unter einem Verteilnetz versteht man ein Netz, das Stoffe, Energie oder Information verteilt. Häufig erstreckt sich ein Verteilnetz über eine geographische Region und dient der Versorgung der Bevölkerung. Solche Verteilnetze sind kritische Infrastrukturen. Viele Staaten haben für Verteilnetzbetreiber spezielle Sicherheitsanforderungen definiert. In Deutschland steht ein IT-Sicherheitsgesetz kurz vor der Verabschiedung, das in erster Linie den Betreibern kritischer Infrastrukturen gewidmet ist. Dort ist vorgesehen, dass diese Betreiber kritischer Infrastrukturen regelmäßig Überprüfungen der Informati-

[11] Vgl. [ISO27000]. S.13
[12] https://www.bsi.bund.de/DE/Themen/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html

onssicherheit der IT-Systeme und Prozesse nachweisen müssen. Daher ist es zweckmäßig ein ISMS einzuführen. Es ist daher insbesondere von aktuellem Interesse ein ISMS-Anwendungsbeispiel aus dem Sektor der Energienetzbetreiber zu wählen.

## Smart Grids

Wir wählen als Anwendungsszenario ein Unternehmen aus dem Sektor Energieversorgung. Zum Steuern des Netzes werden vermehrt zentrale IT-Systeme eingesetzt, also Computersysteme, mit denen man die Energienetzkomponenten überwachen bzw. einstellen kann. Ein Energienetz nennt man *Smart Grid*, wenn die Netzsteuerung durch IT-Systeme unterstützt wird und die Energieerzeuger sowie die Energieverbraucher in die Netzkommunikation einbezogen sind.[13]

## Anwendungsbereich des ISMS

Zum Anwendungsbereich eines Energienetzbetreibers gehören folgende Kernprozesse:

- Stromübertragung
- Netzkopplung
- Zähler- und Anschlussbetrieb
- Störungsmanagement
- Systemdienstleistungen

Gemäß Abbildung 11 unterstützen die Informationssicherheitsprozesse (Tabelle 6) die Geschäftsprozesse bei der Gewährleistung der Informationssicherheit.

## Sicherheitsziele

Infolge der neuen dezentralen Infrastruktur und der daraus resultierenden Peer-to-Peer-artigen Kommunikationsinfrastruktur entstehen für das Energienetz neue IKT-Risiken aufgrund neuer Bedrohungen oder Schwachstellen. Folgende Gefährdungen sind besonders hervorzuheben[14]:

- unbefugte Kenntnisnahme oder Manipulation von Daten, die über das Internet übermittelt werden
- mangelnde Verfügbarkeit von Diensten aufgrund von Denial-of-Service-Attacken oder fehlender „Quality-of-Service“-Optionen
- menschliche Fehlbedienung in komplexen integrierten Netzen

Von großer Bedeutung für den sicheren Betrieb des Verteilnetzes ist der sichere und ordnungsgemäße Betrieb der Leit- und Steuersysteme. Im Einzelnen bedeutet das hauptsächlich:

- Gewährleistung der Informationsvertraulichkeit
- Gewährleistung der Informationsintegrität
- Sicherstellung der Systemverfügbarkeit

Von herausragender Bedeutung ist der Schutz vor unbefugten Modifikationen, also der Schutz der Integrität der Steuerungssysteme. Anderenfalls könnten Netzkomponenten in gefährliche Zustände oder solche, die die Netzverfügbarkeit gefährden können, geführt werden.[15]

[13] [Bund2011], S. 11
[14] Vgl. [VDE2014], S.38f.
[15] Diese Thematik wurde durch den populären Roman „BLACKOUT - Morgen ist es zu spät“ einer breiten Öffentlichkeit zugänglich gemacht.

# 3 Anforderungen an Managementsysteme

***„Die Organisation muss die Informationssicherheitsleistung und die Wirksamkeit des Informationssicherheitsmanagementsystems bewerten."***

ISO/IEC[16]

## 3.1 Informationssicherheitsmanagementsysteme

### ISO/IEC 27001

Die internationale Norm ISO/IEC 27001:2013 definiert Anforderungen an Informationssicherheitsmanagementsysteme. Abschnitt 9.1 thematisiert die Überwachung, Messung, Analyse und Bewertung des ISMS. Im Vordergrund stehen die Anforderungen

- Bewertung der Wirksamkeit des ISMS und
- Bewertung der Informationssicherheitsleistung.

Im Einzelnen wird gefordert[17]:

Die Organisation muss bestimmen:

a) was überwacht und gemessen werden muss, einschließlich der Informationssicherheitsprozesse und Maßnahmen
b) die Methoden zur Überwachung, Messung, Analyse und Bewertung, sofern zutreffend, um gültige Ergebnisse sicherzustellen
c) wann die Überwachung und Messung durchzuführen ist
d) wer überwachen und messen muss
e) wann die Ergebnisse der Überwachung und Messung zu analysieren und zu bewerten sind
f) wer diese Ergebnisse analysieren und bewerten muss.

**Managementprozesse** und **Informationssicherheitsprozesse** stehen in Beziehung zueinander. Die Managementprozesse des ISMS haben den Zweck die Informationssicherheitsprozesse zu planen, zu implementieren, zu bewerten und zu verbessern.

### Beispiele für Informationssicherheitsprozesse gemäß ISO/IEC 27001:2013 (Anhang A)

- Zugangssteuerung
- Handhabung technischer Schwachstellen
- Handhabung von Informationssicherheitsvorfällen

Von einem ISMS wird gemäß Norm erwartet, dass sowohl die Managementprozesse als auch die Informationssicherheitsprozesse gemessen und bewertet werden und dass die zugehörigen Methoden definiert sind und geeignet sind gültige Ergebnisse[18] zu liefern. Messergebnisse sind valide, wenn tatsächlich das gemessen wird, was gemessen werden soll. In der Einleitung wurde mit der Messung der Stromstärke über den Lichtstrom ein invalides Messverfahren präsentiert.

[16] [DIN27001], S. 13 (Abschnitt 9.1)
[17] [ISO27001], S. 13f. (Abschnitt 9.1)
[18] Im englischen Original der Norm ist von „valid results" die Rede.

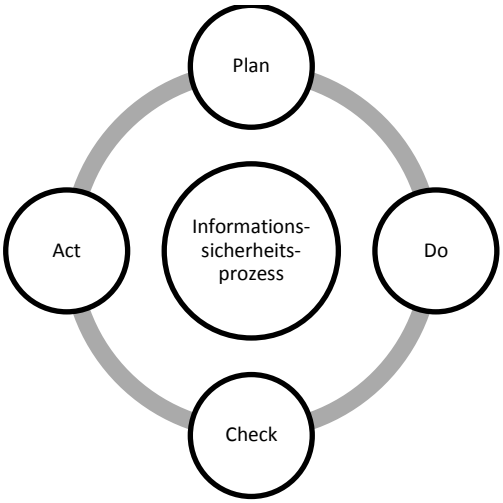


*Abbildung 6: PDCA-Ansatz für Informationssicherheitsprozesse*

Ein wichtiger Erfolgsfaktor für die Wirksamkeit des Managementsystems ist, dass für die Prozesse der Organisation ein „Plan-Do-Check-Act"-Ansatz (PDCA-Ansatz) verfolgt wird.[19]

### ISO/IEC 27004

Die Norm ISO/IEC 27004:2009 gibt Empfehlungen zur Messung des Informationssicherheitsmanagements. Eine zentrale Rolle spielt das „Information security measurement model".[20] Dieses Modell basiert auf dem Messprozess, der in der Norm ISO/IEC 15939:2007, *Systems and software engineering — Measurement process*, veröffentlicht ist. Ausgangspunkt des Prozesses ist die Festlegung der Informationsbedürfnisse. Es sind Informationen, die notwendig sind, um eine Zielkontrolle durchführen zu können.[21] Sie beschreiben den Zweck der Messung. Weitere wichtige Schritte sind die Auswahl der zu messenden Objekte sowie die Festlegung der Maße und der Messmethoden.[22] Am Ende des Messprozesses soll ein Messresultat stehen, das sich aus der Interpretation der Werte der eingeführten Messgrößen ergibt. Die eingeführten Indikatoren werden in der Regel aus Basismaßen oder abgeleiteten Maßen entwickelt.
Das in der Norm dokumentierte Verfahren ist insgesamt stringent, überfordert aber entsprechend der Auditerfahrung des Autors etliche ISMS-Nutzer. Eine zu diesem Thema im Jahr 2014 durchgeführte eigene Umfrage, die an 40 ISMS-Experten und ISMS-Nutzer gerichtet war, zeigte, dass nur 10 Prozent die Norm ISO/IEC 27004:2009 nutzen.

## 3.2 Qualitätsmanagementsysteme

Qualitätsmanagementsysteme haben eine lange Zertifizierungshistorie. Die Norm ISO 9001 mit den entsprechenden Anforderungen steht schon seit 1987 zur Verfügung. Derzeit ist die Version ISO 9001:2008 in Kraft. Auch in dieser Norm sind Anforderungen an das Messen des Managementsystems formuliert.[23] Die ständige Verbesserung der Prozesse des Qualitätsmanagements auf der Grundlage objektiver Messungen ist ein zentrales Element des Managementprozesses.[24] Eine mit „Leistung der Informationssicherheit" (ISO/IEC 27001) vergleichbare Messanforderung findet sich nicht.
ISO 9004 ist ein Leitfaden für das Qualitätsmanagement. Die Norm behandelt unter anderem auch die Themen Messen und Bewerten. Sie gibt zwar keine konkreten Leistungsindikatoren vor, weist aber

[19] [ISO2013], S. 127
[20] [ISO27004], Abschnitt 5.4
[21] [ISO27004], S. 2
[22] [ISO27004], S. 15f.
[23] [ISO9001], S. 39
[24] [ISO9001], S.7

darauf hin, dass entscheidende Leistungskenngrößen (KPI) ermittelt werden sollten. Diese sollten quantifizierbar sein und die Organisation in die Lage versetzen Verbesserungsmaßnahmen zu ergreifen. In diesem Zusammenhang kennt man auch die sogenannte Selbstbewertung.[25]. Diese Selbstbewertung ist im Gegensatz zum internen Audit in der Anforderungsnorm ISO 9001 allerdings nicht erwähnt. Es handelt sich also um eine methodische Zusatzoption und keinen Ersatz für das interne Audit. In Anhang A von ISO 9004 wird insbesondere ein Ansatz zur Ermittlung des Reifegrads einer Organisation vorgestellt. Im nachfolgenden Kapitel wird deutlich, dass der Reifegrad eine Möglichkeit ist die Prozessleistung zu messen.[26] Diese Ausarbeitung konzentriert sich aber auf die Messung der Prozesseffektivität.

## 4 Erfolgsfaktoren für das Messen

Es folgen unterschiedliche Faktoren, die das Messen im Bereich des Informationssicherheitsmanagements verbessern oder erleichtern. Diese werden als Instrumente beim Bewerten der Wirksamkeit des ISMS und der Informationssicherheitsleistung helfen.

### 4.1 Prozesse

Wie bereits geschildert sollten bei Managementsystemen insbesondere Prozesse gemessen werden. Aber dieses Ansinnen ist wenig sinnvoll, wenn nicht präzisiert ist, was gemessen werden soll. Zu den Standard-Leistungsparametern bzw. Schlüsselindikatoren von Prozessen zählen Prozessqualität und Prozesszeit (Durchlaufzeit).[27] Qualität ist der „Grad, in dem ein Satz inhärenter Merkmale Anforderungen erfüllt“.[28] Definieren wir als Prozessziel, dass der Prozess definierte Anforderungen erfüllt, so kann man Prozessqualität als Prozesseffektivität auffassen. Die Durchlaufzeit wird uns weniger beschäftigen, da es in diesem Artikel nicht um Effizienz geht. Weitere Anmerkungen zur Laufzeit der Management- und Informationssicherheitsprozesse werden in Kapitel 5 gemacht.

### 4.2 Ziele

Typisch für die Messung der Prozessleistung ist der Soll-Ist-Vergleich. Hierfür ist die Festlegung von Prozesszielen erforderlich. Bei Managementsystemen bieten sich Ziele der folgenden Kategorien an:

- Effektivität
- Effizienz
- Reifegrad

| | |
|---|---|
| Prozessname | Handhabung von Informationssicherheitsvorfällen |
| Bearbeitungsobjekt | Sicherheitsvorfall |
| Ressourcen | ISMS-Team, Ticketsystem |
| Eingaben | Richtlinie, Verfahrensanweisung |
| Ergebnisse | Minimierter Schaden, Verbesserungsmaßnahmen |
| Besondere Prozessanforderungen | ISO/IEC 27001:2013, Anhang A.16 |

Tabelle 1: Security Incident Management (Beispiel)

[25] [ISO9004], S. 44f.
[26] Wenn der Reifegrad gemessen werden soll, so sollte der Reifegrad des zugehörigen Prozesseses ermittelt werden. Ein klassisches Reifegradmodell ist CMMI® (Capability Maturity Model Integration), das von der Carnegie Mellon University entwickelt wurde. Dort sind Reifegrade für Softwareentwicklungsprozesse definiert und beschrieben. Open Group hat einen Standard veröffentlicht, der einen vergleichbaren Ansatz für Informationssicherheitsprozesse verfolgt. Hier wird der Reifegrad nicht auf einzelne Prozesse, sondern auf das gesamte Prozessensemble bezogen. Zu diesem Zweck werden Fähigkeitsgrade für einzelne Prozesse bestimmt.
[27] [SSE2013], S.158
[28] [ISO9000], S. 18

Für eine Messung der Prozessleistung ist die Definition von Prozesszielen wichtig. Im Beispielfall (Tabelle 1) ist es relativ leicht diese festzulegen, da in Anhang A von ISO/IEC 27001 zu jedem Sicherheitsbereich Maßnahmenziele vorgegeben sind:

### Ziel zu Anhang A.16 Handhabung von Informationssicherheitsvorfällen

***Eine konsistente und wirksame Herangehensweise für die Handhabung von Informationssicherheitsvorfällen einschließlich der Benachrichtigung über Sicherheitsereignisse und Schwächen ist sichergestellt.***

Ziele sollen messbar und spezifisch sein.[29] Für Informationssicherheitsziele fordert ISO/IEC 27001 in Abschnitt 6.2 die Messbarkeit. Ziele sind in der Regel schwer messbar, wenn sie nicht spezifisch sind. Das Ziel in Anhang A.16 ist nicht sehr spezifisch. Allerdings sind in Anhang A zu jedem Ziel konkrete Maßnahmen (Controls) formuliert, die als Indikatoren der Zielerreichung herangezogen werden können. Diese Maßnahmen sind gleichzeitig Forderungen bzw. Anforderungen.

| A.16.1.2 Meldung von Informationssicherheitsereignissen | |
|---|---|
| Titel | Inhalt |
| Meldung von Informationssicherheitsereignissen | Maßnahme<br>Informationssicherheitsereignisse werden so schnell wie möglich über geeignete Kanäle zu deren Handhabung gemeldet. |

*Tabelle 2: Beispiel einer Sicherheitsmaßnahme*

Auf dieser Konkretisierungsstufe können nun präzise Zielvorgaben formuliert werden, zum Beispiel:

Z1: Informationssicherheitsereignisse werden innerhalb von 10 Minuten an den Informationssicherheitsbeauftragten gemeldet.
Z2: Informationssicherheitsereignisse werden nur über sicher verschlüsselte Kommunikationskanäle gemeldet.
Z3: Die Kommunikationskanäle sind verfügbar.

Es kann entschieden werden, ob Ziele wie Z2, in denen noch festzulegende Begriffe („sicher verschlüsselt“) enthalten sind, dadurch eindeutig gemacht werden, dass man den Begriff gleich in der Zielformulierung genauer eingrenzt oder diese Eingrenzung vorab separat vornimmt. Letzteres hat den Vorteil, dass die Formulierung kompakter ist, ersteres hat den Vorteil, dass man unnötigen Interpretationsspielraum vermeidet.

Nun gilt es Maße für die Erreichung der Ziele festzulegen:

Soll die Effektivität der Maßnahme ***A.16.1.2*** bestimmt werden, so sollten Zielerreichungsgrade definiert und gemessen werden. Wichtig ist dabei die erkennbare Festlegung eines Beobachtungszeitraums (z.B. ein Monat).

- Effektivitätsmaß zu Z1: *Anteil der Informationssicherheitsereignisse, die im Zeitraum … innerhalb von 10 Minuten an den Informationssicherheitsbeauftragten gemeldet wurden*
- Effektivitätsmaß zu Z2: *Anteil der Informationssicherheitsereignisse, die im Zeitraum … über sicher verschlüsselte Kommunikationskanäle gemeldet wurden*

Wenn die Effizienz der Maßnahme ***A.16.1.2*** ermittelt werden soll, dann geht es um die Effizienz der diesbezüglich realisierten Methode(n).

- Effizienzmaß 1 zu ***A.16.1.2***: Verfügbarkeit der sicheren Kommunikationskanäle
- Effizienzmaß 2 zu ***A.16.1.2***: Zeitaufwand für die Administration der sicheren Kommunikationskanäle

[29] [DORAN1981], S. 36

## 4.3 Goal Question Metric (GQM)

GQM ist ein Ansatz zum zielorientierten Messen. Victor R. Basili und David Weiss entwickelten diesen Ansatz[30], um das Testen von Software zu professionalisieren. Das Aufschreiben von Fragen (Questions) zu festgelegten Zielen (Goals) erleichtert es, die Ziele in Frageform zu konkretisieren (Operationalisierung) und damit die Zuordnung von Metriken zu erleichtern. Der Ansatz trägt zur Quantifizierung und Objektivierung von relevanten Messvorgängen bei. Weiterhin ermöglicht bzw. erfordert der Ansatz, dass die jeweilige Organisation organisationsspezifische Ziele definiert. Im Idealfall sind die resultierenden Metriken also quantitativ, verfahrensbasiert und organisationsspezifisch.

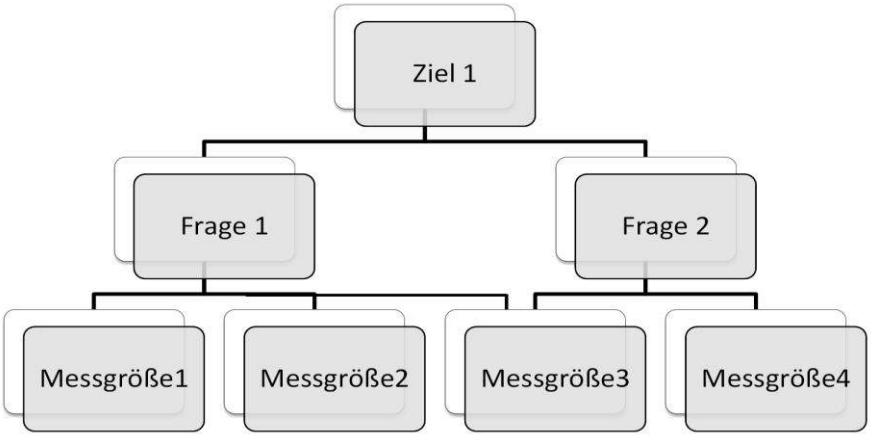


*Abbildung 7: Ausschnitt aus einem GQM-Diagramm, in Anlehnung an [Basi1994, S. 529]*

Der GQM-Ansatz ist relativ simpel. Es ist ein Top-Down-Ansatz, weil die Messungen zielorientiert sein sollen. Diese Ziele sind organisationsspezifische Ziele. Auf der Question-Ebene soll in Frageform formuliert werden, was gemessen werden soll.

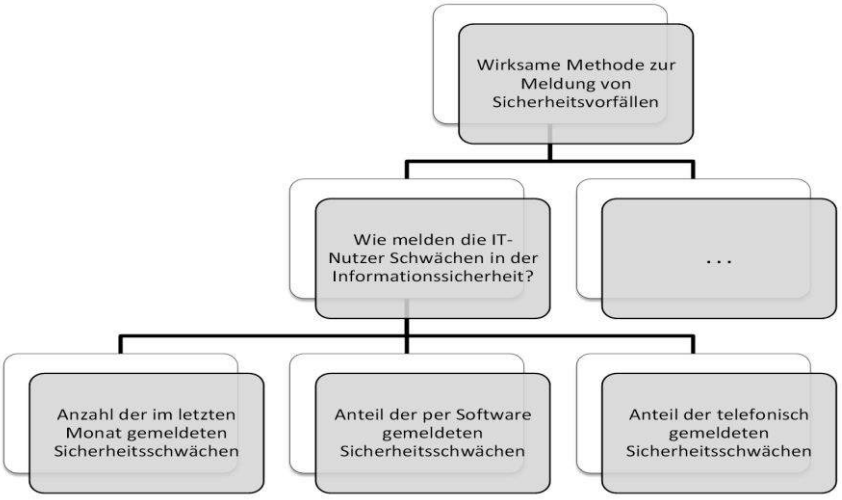


*Abbildung 8: Beispiel eines GQM-Diagramms*

[30] [Basi1982]

## 4.4 Messen mit Metriken

Der GQM-Ansatz liefert ein Verfahren, das es erleichtert angemessene Messgrößen zu finden. Wenn die Messgrößen gefunden sind, dann ist zu klären, wie Messwerte ermittelt werden. Wir betrachten zunächst die folgende binäre Metrik (Distanz):

$$\mathrm{Dist}_2(x,y) = \begin{cases} 0 & wenn\ x = y \\ 1 & wenn\ x \neq y \end{cases}$$

Es wird also nur festgehalten, ob zwei Objektattribute unterschiedlich oder gleich sind. Insbesondere gilt:

$$L_2(\mathrm{x}) = \mathrm{Dist}_2(x,0) = \begin{cases} 0 & wenn\ x = 0 \\ 1 & wenn\ x \neq 0 \end{cases}$$

Man kann $L_2$(x) die „Länge“ von *x* nennen. Es kann für unser Anwendungsgebiet hilfreich sein, alternativ eine dreiwertige, also präzisere Länge für Objekte zu verwenden. Gehen wir davon aus, dass die möglichen x-Werte zwischen 0 und 1 liegen sollen, dann lässt sich definieren:

$$L_3(\mathrm{x}) = \mathrm{Dist}_3(x,0) = \begin{cases} 0 & wenn \quad x = 0 \\ 0{,}5 & wenn \quad x > 0\ und\ x < 1 \\ 1 & wenn \quad x = 1 \end{cases}$$

Diese dreiwertige Länge ermöglicht offensichtlich etwas mehr Differenzierung, die Messungen sind aber immer noch recht einfach. Angelehnt an diese Länge werden nachfolgend ISMS-Messwerte festgelegt.

# 5 Das GQMS-Vorgehensmodell für das Informationssicherheitsmanagement

Abschnitt 9.1 der Norm ISO/IEC 27001:2013 stellt Anforderungen an die Überwachung, Messung, Analyse und Bewertung des ISMS. Im Mittelpunkt stehen die Anforderungen

- Bewertung der Wirksamkeit des ISMS und
- Bewertung der Informationssicherheitsleistung.

Die nachfolgend dargestellten Verfahren sind hilfreiche Etappen auf dem Weg zu einem Mess- und Bewertungsverfahren (PGQM-Verfahren), das prozess- und zielorientiert ist, mithilfe von Zielfragen die Entwicklung von relevanten Messgrößen erleichtert und eine einheitliche Vorgehensweise für die Bewertung des ISMS und der Leistung der Informationssicherheit ermöglicht.

## 5.1 Anforderungsorientiertes Messverfahren

Ein einfaches Messverfahren für den Zustand des ISMS ist das Checklistenverfahren. Der Hauptteil der Norm ISO/IEC 27001 kann als Liste von Anforderungen an das ISMS interpretiert werden. Die Organisation kann im Rahmen eines internen Audits anhand einer Checkliste prüfen, welche Anforderungen erfüllt sind.

| Anforderung | Erfüllungsgrad |
|---|---|
| 5.2 Politik<br>Die oberste Leitung muss eine Informationssicherheitspolitik festlegen, die: | |
| a) für den Zweck der Organisation angemessen ist. | 1 |
| b) Informationssicherheitsziele (siehe 6.2) beinhaltet oder den Rahmen zum Festlegen von Informationssicherheitszielen bietet. | 0,5 |
| . . . | |
| 10.1 Nichtkonformität und Korrekturmaßnahmen<br>Die Organisation muss dokumentierte Information aufbewahren, als Nachweis: | |
| f) der Art der Nichtkonformität sowie jeder daraufhin getroffenen Maßnahme, und | 0,5 |
| g) der Ergebnisse jeder Korrekturmaßnahme. | 0 |
| | |
| Legende: 0 bedeutet: nicht erfüllt; 0,5 bedeutet: teilweise erfüllt; 1 bedeutet: erfüllt | |

*Tabelle 3: Auszug aus ISO/IEC 27001:2013*

Es ist diskussionswürdig, ob für eine Anforderung die Einstufung „teilweise erfüllt“ sinnvoll ist. Ein Auditor prüft bei einem Zertifizierungsverfahren nicht, ob die Anforderungen ein bisschen erfüllt sind. Andererseits ist es gängige Praxis, dass zwischen Hauptabweichungen und Nebenabweichungen unterschieden wird. Eine Anforderung, die überwiegend, aber nicht ganz erfüllt ist, wird in der Regel zu einer Nebenabweichung führen, falls der festgestellte Mangel das Funktionieren des Managementsystems nicht gefährdet. Diese Situation kann mit dem eingeschätzten Wert 0,5 vergleichen.

Benutzt man die Länge $L_3(x)$ in dieser Situation und gehen wir von insgesamt *n* Anforderungen aus, so kann man die Punktsumme

$$S_3 = \mathrm{L}_3(x_1) + \mathrm{L}_3(x_2) + \cdots + L_3(x_n)$$

bilden, so dass der Erfüllungsgrad $E_3 = S_3/n$ (in Prozent) als Indikator für den Zustand des ISMS angesehen werden kann.

**Beispiel (der Einfachheit halber wird n=10 angenommen)**

$$S_3 = 1 + 0 + 0{,}5 + 0{,}5 + 0{,}5 + 0 + 1 + 0{,}5 + 1 + 0{,}5 = 5{,}5\ ;\ E_3 = 55\%$$

Die Formeln berücksichtigen nicht, dass die Anforderungen möglicherweise unterschiedliche Wichtigkeit besitzen. Bei Experten ist es mutmaßlich unstrittig, dass die Anforderung

*6.1.2 Die Organisation muss einen Prozess zur Informationssicherheitsrisikobeurteilung festlegen und anwenden …*

ein stärkeres Gewicht besitzt als die Anforderung

*7.5.2 b) Beim Erstellen und Aktualisieren dokumentierter Information muss die Organisation: … angemessenes Format (z. B. Sprache, Softwareversion, Graphiken) und Medium (z. B. Papier, elektronisches Medium) … sicherstellen.*

Man könnte also eine Punktsumme mit Gewichtung einführen:

$$S_{3g} = g_1 \cdot \mathrm{L}_3(x_1) + g_2 \cdot \mathrm{L}_3(x_2) + \cdots + g_n \cdot L_3(x_n)$$

Andererseits ist es ein schwieriges und insbesondere subjektives Unterfangen, diese Gewichte für die Anforderungen der Norm festzulegen. Es ist nicht klar, ob ein Auditor oder Revisor diese Gewichtungen als plausibel anerkennen wird. Eine Möglichkeit für einen plausiblen Ansatz ist die Berücksichtigung der organisationsspezifischen Sicherheitsziele als Gewichtungskriterium. In diesem Fall würde man die Gewichtungen anhand der Sicherheitsziele der Organisation begründen. Es gibt aber keinen direkten Weg von den dokumentierten Sicherheitszielen zu den Gewichtungen. Weiter unten wird gezeigt, dass der im GQMA-Ansatz eingeschlagene Weg über das Zwischenschalten von Fragen bei der Gewichtung helfen kann.
Beim eben eingeführten Zustandsmaß $E_3$ (Erfüllungsgrad) spielen die Organisationsspezifika keine Rolle. Die Norm fordert in Abschnitt 6.2 aber unmissverständlich, dass die Organisation Informationssicherheitsziele festlegen muss, die die Informationssicherheitsanforderungen berücksichtigt. Außerdem ist die Verwendung des Zustandsmaßes $E_3$ keine befriedigende Reaktion auf die Anforderung, die Effektivität des ISMS zu messen. Denn es ist zu erinnern, dass Effektivität über einen Zielerfüllungsgrad gemessen wird. Wie gesehen, werden aber bei dem anforderungsorientierten Messverfahren (explizit) keine Organisationsziele berücksichtigt.
Außerdem ist zu beachten, dass bei diesem Verfahren die Einschätzung der jeweiligen Erfüllungsgrade intransparent bleibt. Es fehlt eine Messfunktion.

## 5.2 Zielorientiertes Messverfahren

Der ISMS-Betreiber steht vor der Herausforderung, organisationsspezifische Sicherheitsziele für das ISMS festzulegen, und diese sollen möglichst messbar sein.[31]
Der *Goal-Question-Metrik-Ansatz*[32] bietet einen Weg zur Wirksamkeitsmessung, da hierbei Ziele durch Fragen organisationsspezifisch operationalisiert und mit Metriken verknüpft werden.

Als Fallbeispiel soll die Energieverteilung in einem Smart Grid dienen. Das Ziel ist der Norm ISO/IEC 27001:2013 entnommen, also weder organisations- noch branchenspezifisch.

[31] [DIN27001], Abschnitt 6.2
[32] [Basi1994]

| Anwendungsbereich des ISMS: Messen und Steuern des Energieverteilnetzes[33] |
|---|
| Ziel 1 (Z1):<br>5.2 a) ISMS-Politik<br>Die oberste Leitung muss eine Informationssicherheitspolitik festlegen, die für den Zweck der Organisation angemessen ist. |
| Frage 1 (Z11)<br>Beinhaltet die Informationssicherheitspolitik Erwartungen an die Verfügbarkeit der Datenverarbeitungssysteme für die zentrale Leittechnik, die dezentrale Leittechnik sowie die unterstützenden Systeme? |
| Messgröße 1 (M1):<br>Anzahl der schriftlich formulierten Verfügbarkeitserwartungen an die (1) zentrale Leittechnik, (2) die dezentrale Leittechnik sowie (3) die unterstützenden Systeme |
| Frage 2 (Z12)<br>Sind branchenspezifische Gesetze dokumentiert, die unternehmensrelevant sind? |
| Messgröße 2 (M2):<br>Anzahl der dokumentierten branchenspezifischen deutschen Gesetze, die unternehmensrelevant sind |
| Messgröße 3 (M3):<br>Anzahl der branchenspezifischen deutschen Gesetze |
| Messgröße 4 (M4):<br>Anzahl der dokumentierten branchenspezifischen EU-Verordnungen, die unternehmensrelevant sind |
| Messgröße 5 (M5):<br>Anzahl der branchenspezifischen EU-Verordnungen |

*Tabelle 4: GQM-Beispiel – Energienetz - Ziel aus ISO/IEC 27001:2013*

Bei Ziel 1 fällt auf, dass die Formulierung noch relativ vage ist. Dies ist nicht verwunderlich, da es sich um eine Normformulierung handelt, die für alle Organisationen anwendbar sein muss. Mit Hilfe der Fragen gelingt es nun zu konkretisieren, was für das Unternehmen eine angemessene Informationssicherheitspolitik ist. Bei der Energieverteilung spielt die Zuverlässigkeit der Prozessdatenverarbeitung eine zentrale Rolle. Weiterhin unterliegt die Energieversorgungsbranche speziellen gesetzlichen Anforderungen (zum Beispiel das Energiewirtschaftsgesetz). Bei den zugeordneten Metriken fällt auf, dass das Messen hier durchgängig ein Zählen ist. Wie wir unten sehen werden, ist das keineswegs immer der Fall. Wie kann nun aber hier ein Zielerreichungsgrad (Wirksamkeitsmaß) definiert werden?

Der Umgang mit Frage 1 scheint leicht, da nur eine Messgröße $M_1$ zugeordnet ist. Der Wertebereich (hier: 0 bis 3) muss im Messverfahren vermerkt sein. Hier muss von der Organisation eine (subjektive) Zuordnung vorgegeben werden, um ein geeignetes, wenn auch grobes Maß ableiten zu können:

$$ZEG_1 = \begin{cases} 0 & wenn \quad M_1 < 2 \\ 0{,}5 & wenn \quad M_1 = 2 \\ 1 & wenn \quad M_1 = 3 \end{cases}$$

Zu Frage 2 gibt es zwar mehr Messgrößen, aber es ist relativ einfach, ein geeignetes Zielerreichungsmaß abzuleiten, da es das Ziel der Organisation sein sollte, alle relevanten Rechtsvorschriften zu berücksichtigen. So kann man mit Anteilen von unternehmensrelevanten Regulierungen arbeiten:

$$ZEG_2 = (\frac{M_2}{M_3} + \frac{M_4}{M_5})/2$$

[33] Siehe hierzu auch Kapitel 5

Es ist zu beachten, dass die Messgrößen im Nenner Null werden können. In diesem Fall muss der betreffende Summand aus der Formel entfernt werden Ansonsten hat $ZEG_2$ immer Werte zwischen 0 und 1. Man kann also den Erfüllungsgrad von Z12 in Prozent angeben.

Nehmen wir an, dass zum Ziel Z1 tatsächlich nur zwei Fragen Z11 und Z12 existieren, dann kann man für dieses Ziel folgenden Effektivitätsindikator einführen:

$$I_1 = (ZEG_1 + ZEG_2)/2$$

Wenn $ZEG_{1=}$ = 1 und $ZEG_2$ = 1 ist, dann ist auch der Effektivitätsindikator $I_1$ = 1 und somit die Zielerreichung für Z1 100 Prozent.

## 5.3 Prozessorientiertes Messverfahren

Wie schon in Kapitel 1 beschrieben, sind Führung, Planung, Unterstützung, Betrieb, Bewertung und Verbesserung zentrale Elemente eines Managementsystems. Man kann diese Elemente als Prozesse interpretieren.

Die Managementprozesse des ISMS haben den Zweck die Informationssicherheitsprozesse zu planen, zu implementieren, zu bewerten und zu verbessern.

| Kürzel | Bezeichnung |
|---|---|
| M1 | Führung |
| M2 | Planung |
| M3 | Unterstützung |
| M4 | Betrieb |
| M5 | Bewertung |
| M6 | Verbesserung |

*Tabelle 5: Managementprozesse gemäß ISO/IEC 27001:2013*

Eine Anforderung an Managementprozesse ist die kontinuierliche Verbesserung. Das bedeutet die ISMS-Prozesse sollen in erster Linie effektiver werden. Auch die Erhöhung der Effizienz ist immer erwünscht, da Unternehmen wirtschaftlich arbeiten wollen und sollen. Sie steht aber nicht im Fokus dieser Ausarbeitung.[34]

Im Anhang A der Norm ISO/IEC 27001 sind konkretere Anforderungen an Maßnahmen zum Informationssicherheitsmanagement definiert.

| Kürzel | Bezeichnung | Quelle |
|---|---|---|
| I01 | Informationssicherheitsrichtlinien | A.5 |
| I02 | Verwaltung der Sicherheitsorganisation | A.6 |
| I03 | Management der Personalsicherheit | A.7 |
| I04 | Verwaltung der Werte | A.8 |
| I05 | Zugangssteuerung | A.9 |
| I06 | Handhabung der Kryptographie | A.10 |
| I07 | Physische Sicherheit | A.11 |
| I08 | Betriebssicherheit | A.12 |
| I09 | Kommunikationssicherheit | A.13 |

[34] Dieses Thema wird im Artikel von R. Rumpel (Verfahren zur Wirtschaftlichkeitsanalyse von IT-Sicherheitsinvestitionen, e-Journal of Practical Business Research, Berlin, No.10, Berlin 2008, http://www.e-journal-of-pbr.info/downloads/wirtschaftlichkeititsecurityrumpelglanze.pdf), behandelt.

| | | |
|---|---|---|
| I10 | Systementwicklung | A.14 |
| I11 | Lieferantenbeziehungsmanagement | A.15 |
| I12 | Handhabung von Informationssicherheitsvorfällen | A.16 |
| I13 | Business-Continuity-Management | A.17 |
| I14 | Compliancemanagement | A.18 |

*Tabelle 6: Informationssicherheitsprozesse gemäß ISO/IEC 27001:2013 (Anhang A)*

Die Maßnahmenbereiche A.**x** kann man ebenfalls als Prozesse interpretieren: Prozesse sind eine Tätigkeitsstruktur, die eine Eingabe in ein Ergebnis wandeln. Aber was ist das Ergebnis zum Prozess Zugangssteuerung? Und wie lang ist die Durchlaufzeit dieses Prozesses? Eine Anforderung an das ISMS ist das regelmäßige Messen, Überprüfen und Bewerten. Viele ISMS-Anwender bewerten das ISMS einmal jährlich. Dann startet ein neuer Prozessdurchlauf im Rahmen der kontinuierlichen Verbesserung. Der Output am jeweiligen Ende des Prozessdurchlaufs besteht aus den jeweiligen Messergebnissen. Gemessen wird die Effektivität des Prozesses. Die Informationssicherheitsmaßnahmen gemäß ISO/IEC 27001:2013 (Anhang A) erhalten auf diese Weise eine feste Prozessdurchlaufzeit und einen Output.

Man kann also augenscheinlich den diversen Anforderungen der ISMS-Norm ISO/IEC 27001:2013 inklusive Anhang A mit der Einführung von entsprechenden Prozessen begegnen. Insbesondere kann man den Anforderungen[35]

- Bewertung der Wirksamkeit des ISMS und
- Bewertung der Informationssicherheitsleistung

mit einer einheitlichen Methode gerecht werden: Messung der Prozesseffektivität.

## 5.4 Das GQMS-Verfahren

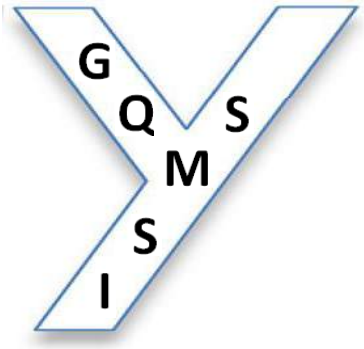


*Abbildung 9: GQMS - Der GQM-Ansatz für ISMS*

Kombiniert man die Prozessorientierung, die Zielorientierung und die Metrikermittlung mittels Fragen (GQM) und wendet diese Prinzipien auf ISMS an, so ergibt sich ein zweckmäßiger und praktikabler Ansatz zur Ermittlung der Effektivität der ISM-Prozesse.
Dieses Verfahren soll anhand von zwei Beispielen verdeutlicht werden.

[35] [ISO27001], Abschnitt 9.1

### 5.4.1 Beispiel 1: Handhabung von Informationssicherheitsvorfällen

| | |
|---|---|
| Prozessname | I12: Handhabung von Informationssicherheitsvorfällen |
| Bearbeitungsobjekt(e) | Sicherheitsvorfall |
| Prozessziel(e) | Eine konsistente und wirksame Herangehensweise für die Handhabung von Informationssicherheitsvorfällen einschließlich der Benachrichtigung über Sicherheitsereignisse und Schwächen ist sichergestellt. |
| Normverweis | ISO/IEC 27001:2013, Anhang A.16 |

*Tabelle 7: Prozessbeispiel (I12)*

#### Ermittlung der Basismessgrößen

Anhang A der Norm erleichtert das Finden von Fragen, da zu den Maßnahmenzielen auch Maßnahmen ausformuliert sind. Die Fragen sind bei dieser Vorgehensweise auf alle Organisationen anwendbar.

| Maßnahme gemäß ISO/IEC 27001:2013, Anhang A.16 | Nr. | Mögliche Frage |
|---|---|---|
| Verantwortlichkeiten und Verfahren<br>Handhabungsverantwortlichkeiten und -verfahren sind festgelegt, um eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle sicherzustellen. | I12_F01 | Welche Handhabungsverantwortlichkeiten sind festgelegt, um eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle sicherzustellen? |
| | I12_F02 | Welche Handhabungsverfahren sind festgelegt, um eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle sicherzustellen? |
| Meldung von Informationssicherheitsereignissen<br>Informationssicherheitsereignisse werden so schnell wie möglich über geeignete Kanäle zu deren Handhabung gemeldet. | I12_F03 | Welche Kanäle werden zur Meldung von Informationssicherheitsereignissen genutzt? |
| | I12_F04 | Sind die Meldekanäle geeignet? |
| | I12_F05 | Wie schnell erfolgt die Meldung? |
| Meldung von Schwächen in der Informationssicherheit<br>Beschäftigte und Auftragnehmer, welche die Informationssysteme und -dienste der Organisation nutzen, werden angehalten, jegliche beobachteten oder vermuteten Schwächen in der Informationssicherheit in Systemen oder Diensten festzuhalten und zu melden. | I12_F06 | Wie melden die IT-Nutzer beobachtete oder vermutete Schwächen in der Informationssicherheit in Systemen oder Diensten? |
| Beurteilung von und Entscheidung über Informationssicherheitsereignisse<br>Informationssicherheitsereignisse werden beurteilt, und es wird darüber entschieden, ob sie als Informationssicherheitsvorfälle einzustufen sind. | I12_F07 | Wie wird entschieden, ob Informationssicherheitsereignisse als Informationssicherheitsvorfälle einzustufen sind? |
| Reaktion auf Informationssicherheitsvorfälle<br>Auf Informationssicherheitsvorfälle wird entsprechend den dokumentierten Verfahren reagiert. | I12_F08 | Wird auf Informationssicherheitsvorfälle entsprechend den dokumentierten Verfahren reagiert? |
| Erkenntnisse aus Informationssicherheits- | I12_F09 | Werden die aus der Analyse und Lösung von Informationssicherheitsvorfällen ge- |

| Maßnahme gemäß ISO/IEC 27001:2013, Anhang A.16 | Nr. | Mögliche Frage |
|---|---|---|
| vorfällen<br>Aus der Analyse und Lösung von Informationssicherheitsvorfällen gewonnene Erkenntnisse werden dazu genutzt, die Eintrittswahrscheinlichkeit oder die Auswirkungen zukünftiger Vorfälle zu verringern. | | wonnenen Erkenntnisse dazu genutzt, die Eintrittswahrscheinlichkeit oder die Auswirkungen zukünftiger Vorfälle zu verringern? |
| Sammeln von Beweismaterial<br>Die Organisation legt Verfahren für die Ermittlung, Sammlung, Erfassung und Aufbewahrung von Information, die als Beweismaterial dienen kann, fest und wendet diese an. | I12_F10 | Ist ein Verfahren für die Ermittlung, Sammlung, Erfassung und Aufbewahrung von Information, die als Beweismaterial dienen kann, festgelegt? |
| | I12_F11 | Wird ein Verfahren für die Ermittlung, Sammlung, Erfassung und Aufbewahrung von Information, die als Beweismaterial dienen kann, angewendet? |

*Tabelle 8: Fragen zum Prozess I12 gemäß GQM-Ansatz*

Nun gilt es den Fragen möglichst quantitative Messgrößen zuzuordnen. Hinweise hierfür liefert die Norm ISO/IEC 27002:2013. Weiterhin können bzw. sollten hier unternehmens- bzw. branchenspezifische Aspekte berücksichtigt werden. Insbesondere ist die Ermittlung der Messwerte eine unternehmensbezogene Aufgabe. Die Bedingungen, nach denen in Tabelle 9 das 3-Wert-Clustering vorgenommen wurde, sind abhängig von den Sicherheitsprioritäten und Sicherheitszielen der Organisation und sollten mit diesen konsistent sein. Das Clustern der Messwerte stellt eine unternehmensinterne Entscheidung dar und kann als implizite Gewichtung angesehen werden. Es ist auf Sorgfalt und Nachvollziehbarkeit zu achten. Für die Energienetzbetreiber kann zum Ermitteln der Messgrößen auch der Standard ISO/IEC TR 27019 hilfreich sein, in dem energieversorgungsspezifische Maßnahmen in Anlehnung an ISO/IEC 27002 festgehalten sind.

| Nr. | Mögliche Frage | Nr. | Messgröße | Messwert |
|---|---|---|---|---|
| I12_F01 | Welche Handhabungsverantwortlichkeiten sind festgelegt, um eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle sicherzustellen? | I12_F01_M01 | Anzahl der Handhabungsverantwortlichen für die Vorfallreaktion | 0 wenn I12_F01_M01=0<br>0,5 wenn I12_F01_M01=1<br>1 wenn I12_F01_M01>1 |
| I12_F02 | Welche Handhabungsverfahren sind festgelegt, um eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle sicherzustellen? | I12_F02_M01 | Anzahl der Verfahren für die Reaktion auf Sicherheitsvorfälle | 0 wenn I12_F02_M01=0<br>1 wenn I12_F02_M01>0 |
| | | I12_F02_M02 | Durchschnittliche Reaktionsdauer auf Sicherheitsvorfälle im letzten Monat | 0 wenn I12_F02_M02 > 24h<br>0,5 wenn I12_F02_M02 ≤ 24h, aber größer als 12 h<br>1 wenn I12_F02_M02 ≤ 12 h |

| Nr. | Mögliche Frage | Nr. | Messgröße | Messwert |
|---|---|---|---|---|
| | | I12_F02_M03 | Anteil der Sicherheitsvorfälle, die von einem Fachexperten bearbeitet wurden | 0 wenn I12_F02_M03 < 50%<br>0,5 wenn I12_F02_M03 ≥ 50%, aber kleiner als 80%<br>1 wenn I12_F02_M03 ≥ 80% |
| I12_F03 | Welche Kanäle werden zur Meldung von Informationssicherheitsereignissen genutzt? | I12_F03_M01 | Anzahl der Meldekanäle | 0 wenn I12_F03_M01 = 0<br>0,5 wenn I12_F03_M01 = 1<br>1 wenn I12_F03_M01 ≥ 1 |
| | | I12_F03_M02 | Anteil der elektronischen Meldekanäle | 0 wenn I12_F03_M02 = 0<br>1 wenn I12_F03_M02 > 0 |
| I12_F04 | Sind die Meldekanäle geeignet? | I12_F04_M01 | Anteil der Meldekanäle mit sicherer Verschlüsselung | 0 wenn I12_F04_M01 = 0<br>0,5 wenn I12_F04_M01 > 0<br>1 wenn I12_F04_M01 = 1 |
| I12_F05 | Wie schnell erfolgt die Meldung? | I12_F05_M01 | Durchschnittliche Dauer vom Eintritt des Sicherheitsereignisses bis zur schriftlichen Meldung im letzten Monat | 0 wenn I12_F05_M01 > 12 h<br>0,5 wenn I12_F02_M02 ≤ 12h, aber größer als 6 h<br>1 wenn I12_F05_M01 < 6 h |
| I12_F06 | Wie melden die IT-Nutzer beobachtete oder vermutete Schwächen in der Informationssicherheit in Systemen oder Diensten? | I12_F06_M01 | Anzahl der im letzten Monat gemeldeten Sicherheitsschwächen | … |
| | | I12_F06_M02 | Anteil der schriftlich gemeldeten Sicherheitsschwächen | … |
| | | I12_F06_M03 | Anteil der per Störungsmanagementsoftware gemeldeten Sicherheitsschwächen | … |
| | | I12_F06_M04 | Anteil der telefonisch gemeldeten Sicherheitsschwächen | … |
| I12_F07 | Wie wird entschieden, ob Informationssicherheitsereignisse als Informationssi- | I12_F07_M01 | Anzahl der im letzten Monat gemeldeten Sicherheitsereignisse | … |

| Nr. | Mögliche Frage | Nr. | Messgröße | Messwert |
|---|---|---|---|---|
| | cherheitsvorfälle einzustufen sind? | I12_F07_M02 | Anteil der im letzten Monat gemeldeten Sicherheitsereignisse, die von gemäß Sicherheitsvorfallverfahren als Informationssicherheitsvorfall eingestuft wurden | … |
| I12_F08 | Wird auf Informationssicherheitsvorfälle entsprechend den dokumentierten Verfahren reagiert? | I12_F08_M01 | Anzahl der im letzten Monat als Sicherheitsvorfall eingestuften Ereignisse | … |
| | | I12_F08_M02 | Anteil der Sicherheitsvorfälle, bei denen Reaktionsaktivitäten in angemessenem Umfang schriftlich dokumentiert sind | … |
| | | I12_F08_M03 | Anteil der Sicherheitsvorfälle, bei denen die Reaktion zu einer Verringerung der Verwundbarkeit geführt hat | … |
| I12_F09 | Werden die aus der Analyse und Lösung von Informationssicherheitsvorfällen gewonnenen Erkenntnisse dazu genutzt, die Eintrittswahrscheinlichkeit oder die Auswirkungen zukünftiger Vorfälle zu verringern? | I12_F09_M01 | Anteil der Sicherheitsvorfälle, bei denen die Reaktion zu einer Verringerung der Eintrittswahrscheinlichkeit zukünftiger Vorfälle geführt hat. | … |
| | | I12_F09_M02 | Anteil der Sicherheitsvorfälle, bei denen die Reaktion zu einer Verringerung der Schadensauswirkung zukünftiger Vorfälle geführt hat | … |
| I12_F10 | Ist ein Verfahren für die Ermittlung, Sammlung, Erfassung und Aufbewahrung von Information, die als Beweismaterial dienen kann, festgelegt? | I12_F10_M01 | Anzahl der Seiten, auf denen das Verfahren für die Ermittlung, Sammlung, Erfassung und Aufbewahrung von Information, die als Beweismaterial dienen kann, festgelegt ist | … |
| I12_F11 | Wird ein Verfahren für die Ermittlung, Sammlung, Erfassung und Aufbewahrung von Information, die als Beweismaterial dienen kann, angewendet? | I12_F11_M01 | Anzahl der Sicherheitsvorfälle, bei denen verfahrensgemäß Information, die als Beweismaterial dienen kann, gesammelt und erfasst werden müsste | … |
| | | I12_F11_M02 | Anteil der Sicherheitsvorfälle, bei denen verfahrensgemäß Information, die als Beweismaterial dienen kann, gesammelt und erfasst worden ist | … |

*Tabelle 9: Messgrößen zum Prozess I12 gemäß GQM-Ansatz*

In Kapitel 3 wurde die dreiwertige Länge $L_3(x)$ eingeführt. In ähnlicher Weise wurden in Tabelle 9 die möglichen Messwerte festgelegt. Natürlich ist es auch denkbar und möglich, eine differenziertere Ratingskala zu verwenden, also eine Skala mit vier oder mehr Werten. Wenn es um Messgrößen mit subjektivem Interpretationsspielraum geht (wie zum Beispiel *I12_F08_M02 Anteil der Sicherheitsvorfälle, bei denen Reaktionsaktivitäten in angemessenem Umfang schriftlich dokumentiert sind*), kann eine solche Verfeinerung allerdings zu neuen Schwierigkeiten führen, da sich die Gefahr einer fehlerhaften Wertzuweisung und der Diskussionsaufwand erhöht. Die hier verwendete dreiwertige, normierte Skala ist als Vorschlag zu verstehen.
Um eine Messung vollständig zu definieren, sollten das Messverfahren, die Messungsfrequenz, die Maßeinheit und die Zielwerte definiert sein.

**Beispiel: I12_F02_M02 / Durchschnittliche Reaktionsdauer auf Sicherheitsvorfälle**

- Messungsfrequenz: monatlich
- Maßeinheit: Stunde (h)
- Zielwert: Durchschnittliche Reaktionsdauer höchstens 12 h
- Messverfahren: Wird ein Informationssicherheitsereignis als ein Informationssicherheitsvorfall eingestuft, so wird das im Störungsmanagementsystem dokumentiert. Es ist also feststellbar, wann diese Einstufung vorgenommen wurde. Der Zeitpunkt der Reaktion ist definiert als der Zeitpunkt, an dem im Störungsmanagementsystem eine zugehörige Aktivität dokumentiert wurde. Aktivitäten können sein: Zuweisung des Vorgangs an einen Fachexperten, operative Aktivität durch den Bearbeiter selbst, Rückfrage an den Melder usw. Die Reaktionsdauer wird festgelegt als die Differenz von Reaktionszeitpunkt und Einstufungszeitpunkt

Es wird deutlich, dass die Beschreibung des Messverfahrens erheblichen Einfluss auf das Messergebnis hat. Ist das Messverfahren nicht oder nur knapp beschrieben, kann es durch den Interpretationsspielraum zu deutlich abweichenden Ergebnissen kommen.
Beim Prozess I12 wurden insgesamt 22 Messgrößen definiert. Wie ist nun aber die Effektivität des Prozesses insgesamt einzuschätzen?

## Abgeleitete Maße

Es ist zielführend gemäß GQMS-Verfahren fragenorientiert vorzugehen, d.h. für jede Frage eine abgeleitete Messgröße festzulegen. Die abgeleiteten Messgrößen können zu einem Prozessindikator kombiniert werden. Falls es zu einer Frage nur eine Messgröße gibt, so ist die Herleitung eines Ableitungsmaßes nicht erforderlich, sondern die Basismessgröße kann gleichzeitig als abgeleitete Messgröße angesehen werden.

## Beispiel: Frage I12_F01

Die einzige Messgröße ist I12_F01_M01. Dementsprechend ist die abgeleitete Messgröße

*A_I12_F01 = I12_F01_M01*

## Beispiel: Frage I12_F02

Die zugeordneten Messgrößen sind: *I12_F02_M01*, *I12_F02_M02* und *I12_F02_M03*. Sie sind normiert, da das dreiwertige Maß $L_3(x)$ verwendet wird.

Da alle drei Größen voneinander unabhängige Qualitätsmerkmale repräsentieren, ist als Ableitungsmaß geeignet:

*A_I12_F02 = I12_F02_M01 + I12_F02_M02 + I12_F02_M03.*

Auch hier ist die Frage nach der Gewichtung gerechtfertigt. Es handelt sich um eine subjektive Einschätzung der Bedeutung der Messgrößen. Wenn man davon ausgeht, dass keine der Messgrößen höhere Priorität als die anderen hat, kann das Ableitungsmaß bleiben, wie es ist.

## Indikatoren

Unter dieser Voraussetzung kann man den Effektivitätsindikator des Prozesses I12 ermitteln, indem man alle abgeleiteten Maße zu den Fragen summiert:

$$Eff(I12) = A\_I12\_F01 + A\_I12\_F02 + \ldots + A\_I12\_F11.$$

Dieses Maß ist noch nicht normiert, das heißt noch nicht auf den Wertebereich [0,1] skaliert. Maße mit absoluten Werten kann man untereinander nicht ohne weiteres vergleichen. *Eff(I12)* kann Werte zwischen 0 und 22 annehmen, da ja insgesamt 22 Messwerte erhoben werden. Bei einem anderen Prozess werden vielleicht nur 13 Messwerte erhoben. Somit kann maximal der Wert 13 angenommen werden. Das heißt aber nicht, dass dieses Ergebnis dann auf geringere Effektivität hinweist. Die Normierung kann man vornehmen, indem man *Eff(I12)* durch die Anzahl aller Basismessgrößen des Prozesses, die als Summanden in die Ableitungsmaße einfließen, dividiert, da die Basismessgrößen selbst normiert sind:

$$Eff_n(I12) = (A\_I12\_F01 + A\_I12\_F02 + \ldots + A\_I12\_F11) / 22.$$

Es ist möglich, dass eine Basismessgröße bei mehreren Ableitungsmaßen als Summand eingeht. Dann ist mehrfach zu zählen Der normierte Effektivitätsindikator $Eff_n(I12)$ kann nur noch Werte zwischen 0 und 1 annehmen. Beispielsweise ist $Eff_n(I12)$ = 0,68, das entspricht 59%. Der Prozess I12 hat also eine Effektivität (Zielerreichungsgrad) von 59%. Auf diese Art und Weise kann man die Effektivität von Prozessen sinnvoll vergleichen.

Es wurde auch hier keine Gewichtung vorgenommen. Gibt es einleuchtende, organisationsspezifische Begründungen, die Anlass geben, bestimmte Fragen höher zu gewichten, so kann man Gewichtungen einführen. Der Einfachheit halber sollte man mit ganzzahligen Gewichtungen $g_i \in \mathbb{Z}$ arbeiten. Dann kann man die gewichtete Effektivität wie folgt bestimmen:

$$Eff\_g(I12) = g_1*A\_I12\_F01 + g_2*A\_I12\_F02 + \ldots + g_{11}*A\_I12\_F11.$$

Um die Normierung zu erreichen, ist folgende Berechnung erforderlich:

$$\boldsymbol{Eff\_g_n(I12) = (g_1*A\_I12\_F01 + g_2*A\_I12\_F02 + \ldots + g_{11}*A\_I12\_F11) / (g_1 + g_2 + \ldots + g_{11})}$$

## Beispiel zur Berechnung der Prozesswirksamkeit

Ohne Gewichtung ergibt sich:

$$Eff(I12) = 1+0,5+0,5+0+1+1+0,5+0,5+1+0,5+1 = 6,5.$$
$$Eff_n(I12) = (1+0,5+0,5+0+0+1+0,5+0,5+1+0,5+1) / 11 = 0,591.$$

Wird eine Gewichtung vorgenommen, so kann sich der Wert des Effektivitätsindikators deutlich verändern:

$$Eff\_g(I12) = 1*1+2*0,5+1*0,5+1*0+2*1+1*1+1*0,5+1*0,5+1*1+2*0,5+1*1 = 9,5.$$
$$\boldsymbol{Eff\_g_n(I12) = (Eff\_g(I12)) / 14 = 0,679.}$$

Der Prozess hat eine gewichtete, normierte Effektivität von 67,9%.

Der Prozess hat eine ungewichtete, normierte Effektivität von 59,1%. Die Gewichtung kann also einen beachtlichen Einfluss auf das Effektivitätsergebnis haben. Je mehr Fragen mit erhöhtem Gewicht ausgestattet werden, desto stärker können die Ergebnisse voneinander abweichen.

Für Managementprozesse ist die geschilderte Vorgehensweise ähnlich. Ein wichtiger Unterschied besteht allerdings darin, dass die Fragen nicht so leicht abzuleiten sind, da ein Gerüst von formulierten Maßnahmen wie bei den Informationssicherheitsprozessen fehlt.

### 5.4.2 Beispiel 2: Verwaltung der Werte

Gemäß ISO/IEC 27001:2013, Anhang A.8 besteht die Verwaltung der Werte[36] aus folgenden Maßnahmenbereichen:

- A.8.1 Verantwortlichkeit für Werte
- A.8.2 Informationsklassifizierung
- A.8.3 Handhabung von Datenträgern

Die Wertobjekte, um die es hier geht, sind hauptsächlich Informationen und IT-Systeme. Bei den IT-Systemen ist es sinnvoll zwischen Software und Hardware zu differenzieren. Bei der Erfassung für das ISMS, insbesondere die Risikobewertung, sollten die Assets zu Gruppen gleichartiger Objekte zusammengefasst werden. Beispiele für Wertobjekte im ISMS für Energienetze finden sich in Tabelle 10:

| Kategorie: | Information | Software | Hardware |
|---|---|---|---|
| Beispiel 1 | Prozessvisualisierungsdaten | Visualisierungs-software | PC |
| Beispiel 2 | Zustandsdaten; Konfigurationsdaten | Projektierungssoftware | PC |
| Beispiel 3 | Meldungen; Zählwerte; Messwerte; Steuerbefehle | Fernwirksystem | Mittelspannungsfeldgerät |

*Tabelle 10: Wertobjekte der Prozesssteuerung / Netzleittechnik (Auswahl)*

Anhang *A.8 (Verwaltung der Werte)* entspricht gemäß Tabelle 6 dem Prozess I04. Für den Teilprozess I04/1 (entspricht *A.8.1 Verantwortlichkeit für Werte*) sollen im Folgenden die Basismessgrößen definiert werden.

| | |
|---|---|
| Prozessname | I04/1: Verantwortlichkeit für Werte |
| Bearbeitungsobjekt(e) | Wertobjekt |
| Prozessziel(e) | Die Werte der Organisation sind identifiziert und angemessene Verantwortlichkeiten zu ihrem Schutz sind festgelegt. |
| Normverweis | ISO/IEC 27001:2013, Anhang A.8 |

*Tabelle 11: Prozessbeispiel (I04, entspricht Teilprozess A.8.1)*

[36] Im Originaltext wird das Wort „Asset“ verwendet.

Zunächst werden gemäß GQM-Ansatz zu den in der Norm ISO/IEC 27001:2013 Anhang A vorgegebenen Zielen Fragen formuliert.

| Maßnahme gemäß ISO/IEC 27001:2013, Anhang A.8 | Nr. | Mögliche Frage |
|---|---|---|
| Inventarisierung der Werte<br>Information und andere Werte, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sind erfasst und ein Inventar dieser Werte ist erstellt und wird gepflegt. | I04_F01 | Sind die im Einsatz befindlichen PDV-Systeme im Inventarverzeichnis dokumentiert? |
| | I04_F02 | Sind im Inventarverzeichnis neben den Hardwareobjekten auch die zugehörigen Softwareobjekte und die dort verarbeiteten Informationen dokumentiert? |
| | I04_F03 | Wird das Inventarverzeichnis regelmäßig aktualisiert und ergänzt? |
| Zuständigkeit für Werte<br>Für alle Werte, die im Inventar geführt werden, gibt es Zuständige. | I04_F04 | Gibt es für alle im Einsatz befindlichen PDV-Systeme Zuständige? |
| Zulässiger Gebrauch von Werten<br>Regeln für den zulässigen Gebrauch von Information und Werten, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sind aufgestellt, dokumentiert und werden angewendet. | I04_F05 | Existieren Regeln für den zulässigen Gebrauch von PDV-Systemen? |
| | I04_F06 | Sind Regeln für den zulässigen Gebrauch von PDV-Systemen dokumentiert? |
| | I04_F07 | Werden die Regeln für den zulässigen Gebrauch von PDV-Systemen angewendet? |
| Rückgabe von Werten<br>Alle Beschäftigten und sonstige Benutzer, die zu externen Parteien gehören, geben bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung sämtliche in ihrem Besitz befindlichen Werte, die der Organisation gehören, zurück. | I04_F08 | Geben die Beschäftigten bei Beendigung des Beschäftigungsverhältnisses sämtliche in ihrem Besitz befindlichen Werte, die der Organisation gehören, zurück? |
| | I04_F09 | Geben die externen Benutzer bei Beendigung des Vertragsverhältnisses sämtliche in ihrem Besitz befindlichen Werte, die der Organisation gehören, zurück? |

*Tabelle 12: Fragen zu den Zielen des Teilprozesses I04/1 von Prozess I04 Verwaltung der Werte*

Nun kann man anhand der formulierten Fragen Messgrößen festlegen, die zum Unternehmen passen. Auch hier sind die genannten Kriterien für die Zuweisung von Messwerten folglich nur Vorschläge. In Tabelle 13 sind exemplarisch Messgrößen und Messwerte aufgeführt.

| Nr. | Mögliche Frage | Nr. | Messgröße | Messwert |
|---|---|---|---|---|
| I04_F01 | Sind die im Einsatz befindlichen PDV-Systeme im Inventarverzeichnis dokumentiert? | I04_F01_M01 | Anteil der im Einsatz befindlichen PDV-Hardwareobjekte, die im Inventarverzeichnis dokumentiert sind | 0, wenn I04_F01_M01 < 80%<br>0,5 wenn I04_F01_M01 ≥ 80%, aber kleiner als 95%<br>1 wenn I04_F01_M01 ≥ 95% |
| I04_F02 | Sind im Inventarverzeichnis neben den Hardwareobjekten auch die zugehörigen | I04_F02_M01 | Anteil der im Einsatz befindlichen PDV-Softwareobjekte, die im | 0, wenn I04_F02_M01 < |

| Nr. | Mögliche Frage | Nr. | Messgröße | Messwert |
|---|---|---|---|---|
| | Softwareobjekte und die dort verarbeiteten Informationen dokumentiert? | | Inventarverzeichnis dokumentiert sind | 80%<br>0,5 wenn I04_F02_M01 ≥ 80%, aber kleiner als 95%<br>1 wenn I04_F02_M01 ≥ 95% |
| | | I04_F02_M02 | Anteil der im Inventarverzeichnis dokumentierten PDV-Softwareobjekte, bei denen die verarbeiteten Informationen ausgewiesen sind | 0, wenn I04_F01_M02 < 80%<br>0,5 wenn I04_F01_M02 ≥ 80%, aber kleiner als 95%<br>1 wenn I04_F01_M02 ≥ 95% |
| I04_F03 | Wird das Inventarverzeichnis regelmäßig aktualisiert und ergänzt? | I04_F03_M01 | Anzahl der im Berichtszeitraum nachgewiesenen Aktualisierungen? | 0 wenn I04_F03_M01 <2<br>0,5 wenn I04_F03_M01 ≥ 2 aber kleiner als 4<br>1 wenn<br>I04_F03_M01 ≥ 4 |
| | | I04_F03_M02 | Anteil der im Berichtszeitraum nachgewiesenen Ergänzungen | 0 wenn I04_F03_M02=0<br>1 wenn I04_F03_M02 > 0 |
| I04_F04 | Gibt es für alle im Einsatz befindlichen PDV-Systeme Zuständige? | I04_F04_M01 | … | … |
| I04_F05 | Existieren Regeln für den zulässigen Gebrauch von PDV-Systemen? | I04_F05_M01 | … | … |
| I04_F06 | Sind Regeln für den zulässigen Gebrauch von PDV-Systemen dokumentiert? | I04_F06_M01 | … | … |
| | | I04_F06_M02 | … | … |
| | | I04_F06_M03 | … | … |
| | | I04_F06_M04 | … | … |
| I04_F07 | Werden die Regeln für den zulässigen Gebrauch von PDV-Systemen angewendet? | I04_F07_M01 | … | … |
| | | I04_F07_M02 | … | … |
| I04_F08 | Geben die Beschäftigten bei Beendigung des Beschäftigungsverhältnisses sämtliche in ihrem Besitz befindli- | I04_F08_M01 | … | … |
| | | I04_F08_M02 | … | … |

| Nr. | Mögliche Frage | Nr. | Messgröße | Messwert |
|---|---|---|---|---|
| | chen Werte, die der Organisation gehören, zurück? | I04_F08_M03 | … | … |
| I04_F09 | Geben die externen Benutzer bei Beendigung des Vertragsverhältnisses sämtliche in ihrem Besitz befindlichen Werte, die der Organisation gehören, zurück? | I04_F09_M01 | … | … |
| | | I04_F09_M02 | … | … |

*Tabelle 13: Messgrößen zum Prozess I04/1 Verantwortlichkeit für Werte gemäß GQM-Ansatz*

Das Ableitungsmaß für den Teilprozess *I04/1 (Verantwortlichkeit für Werte)* ergibt sich in analoger Weise wie in Beispiel 1.

## 5.5 Bewertung des ISMS

Die normierten Prozesseffektivitätskennzahlen kann man anschaulich mit Spinnennetzdiagrammen vergleichen. Ein Abbildung 10 entsprechendes Diagramm kann man auch für den Bereich der Informationssicherheitsprozesse erstellen.

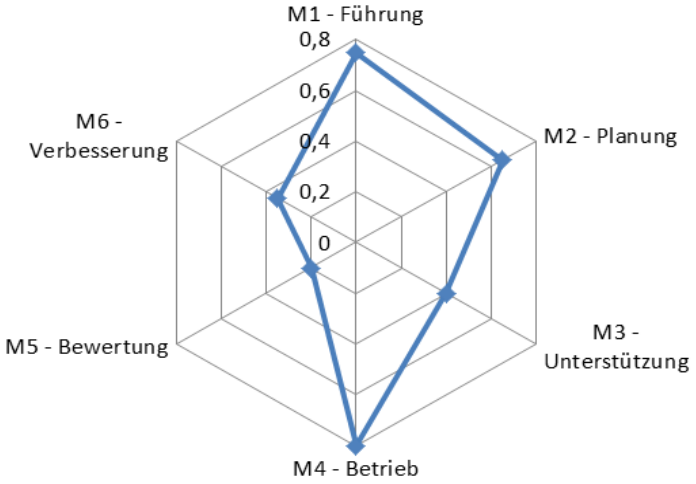


*Abbildung 10: Veranschaulichung der Effektivität der Managementprozesse*

Wie gesehen, gibt es insgesamt 6 Managementprozesse M1 bis M6 und 14 Informationssicherheitsprozesse I1 bis I14. Da die Effektivitätsindikatoren $Eff\_g_n()$ normiert sind, lässt sich recht einfach die normierte Gesamteffektivität des Managementsystems (MS) und des Prozessportfolios für das Informationssicherheitsmanagements (ISM) ermitteln:

$$Eff_n(MS) = (Eff\_g_n(M1) + \ldots Eff\_g_n(M6)) / 6$$

$$Eff_n(ISM) = (Eff\_g_n(I01) + Eff\_g_n(I02) + \ldots Eff\_g_n(I14)) / 14$$

Aufgrund der organisationsspezifischen Fragen, Metriken, Zielwerte und Ableitungsmaße handelt es sich bei diesen Spitzenkennzahlen um organisationsspezifische Effektivitätsmaße. Die Ergebnisse sind also nicht ohne weiteres mit anderen Organisationen vergleichbar. Dennoch ist ein Vergleich ähnlicher Organisationen grundsätzlich sinnvoll und möglich, wenn dasselbe Messverfahren verwendet wurde.

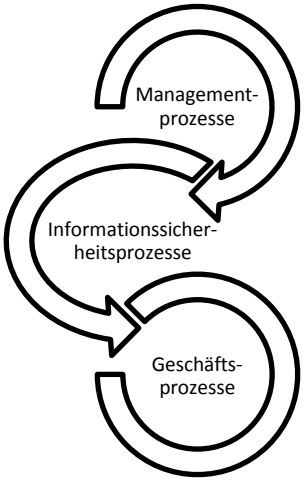


*Abbildung 11: Prozessgebiete des ISMS*

Auch bei den Spitzenkennzahlen kann man erneut die Frage nach der Gewichtung aufwerfen. Ein plausibler Ansatz besteht darin, die Auswirkungen der Management- und Informationssicherheitsprozesse auf die Geschäftsprozesse der Organisation einzuschätzen. Die Managementsystemprozesse unterstützen die Informationssicherheitsprozesse hinsichtlich der kontinuierlichen Verbesserung. Die Informationssicherheitsprozesse unterstützen die Geschäftsprozesse bei der Gewährleistung der Informationssicherheit. Es ist sinnvoll, dass bei der Gesamtbewertung des ISMS diejenigen Prozesse stärker gewichtet werden, die mehrere Geschäftsprozesse unterstützen. Auf der anderen Seite wäre beispielsweise der Prozess *I06 Handhabung der Kryptographie* gering zu gewichten, wenn die zum Anwendungsbereich des ISMS gehörenden Geschäftsprozesse gar keine Verschlüsselung benötigen, da Vertraulichkeit kein relevantes Sicherheitsziel des ISMS der Organisation ist, sondern Verfügbarkeit und Integrität im Vordergrund stehen. Ist für die Prozesse eine plausible Gewichtung vorgenommen worden, so ist es möglich und vertretbar eine Gesamteffektivitätskennzahl für alle 20 Prozesse zu bestimmen.

### 5.6 Kurzfassung des GQMS-Vorgehensmodells

1. *Die Kapitel des Hauptteils der Norm ISO/IEC 27001 als Prozesse definieren*
2. *Die Kapitel des Anhangs A der Norm ISO/IEC 27001 als Prozesse definieren*
3. *Den Prozessen des Hauptteils per GQM-Ansatz Ziele, Fragen und Metriken zuordnen*
4. *Den Prozessen des Anhangs A als Ziele die Maßnahmenziele des Anhang A zuordnen und die Fragen anhand der Maßnahmen aus Anhang A stellen; anhand der Fragen normierte Basismessgrößen samt Zielwerten entwickeln*
5. *Aus den Basismessgrößen durch Summierung abgeleitete Maße für die Fragen erzeugen; gegebenenfalls gewichtete Summen bilden*
6. *Durch Summierung der abgeleiteten Maße Effektivitätsindikatoren für den Prozess erzeugen; Indikator normieren; gegebenenfalls gewichtete Summen bilden*
7. *Durch Summierung der Effektivitätsindikatoren für die Prozesse und Normierung Effektivitätsindikatoren für die Prozessgebiete Managementsystem und Informationssicherheitsmanagement erzeugen*

## 6 Fazit

Die erste Forschungsfrage war: *Ist es möglich einen quantitativen Effektivitätsindikator für ISMS systemunabhängig herzuleiten?* Es hat sich herausgestellt, dass das Verfahren zur Ableitung des Effektivitätsindikators tatsächlich systemunabhängig anwendbar ist. Andererseits ist das Vorgehen zur Be-

stimmung der Messwerte der Messgrößen system- bzw. organisationsabhängig. Das ist nicht bedauerlich, sondern wichtig für die Relevanz der Ergebnisse. Letzten Endes geht es darum, dass eine Organisation die Anforderungen der Norm ISO/IEC 27001 erfüllen möchte oder muss. Beispielsweise fordert *A.16.1.1 Verantwortlichkeiten und Verfahren* folgende Maßnahme:

*Handhabungsverantwortlichkeiten und -verfahren sind festgelegt, um eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle sicherzustellen.*

Man sieht, dass die Anforderung nicht im Detail fordert, wie viele Handhabungsverantwortliche die Organisation vorweisen muss. Andererseits wird aus der Formulierung klar, dass die Verantwortlichkeit festgelegt sein muss.
Es ist also nicht fahrlässig, sondern angemessen, beim Festlegen der Messwerte Entscheidungsspielraum für den ISMS-Anwender zu lassen. Allerdings müssen die Entscheidungen immer so gestaltet sein, dass die Erfüllung der Anforderungen durch das Messwertcluster angemessen widergespiegelt ist.
Die zweite Forschungsfrage lautete: *Ist das zugehörige Vorgehensmodell eine solide und verständliche theoretische Grundlage für das Messen, Analysieren und Bewerten der Effektivität von ISMS, dessen Anwendbarkeit und Verständlichkeit ausreichend ist, um beträchtliche Akzeptanz bei den Zielgruppen zu erreichen?* Das Verfahren zur Ermittlung der Wirksamkeit steht auf folgenden bewährten Säulen: Prozessorientierung, GQM-Ansatz, international anerkannte Norm, Rechenverfahren zur Normierung. Es ist möglich, mit den Indikatoren $Eff_n(MS)$ und $Eff_n(ISM)$ die Effektivität des ISMS und die Informationssicherheitsleistung zu bewerten. An Beispielen wurde die Anwendbarkeit nachgewiesen. Ob das GQMS-Modell hinreichend verständlich ist, um beträchtliche Akzeptanz bei den Zielgruppen (ISMS-Anwender, ISMS-Berater) zu erreichen, können nur die Mitglieder der Zielgruppen einschätzen.
Das Verfahren erleichtert es dem ISMS-Anwender, die erforderlichen Messungen so vorzunehmen, dass die ISMS-Verantwortlichen gezielter Verbesserungen vornehmen und Revisoren bzw. Auditoren den Zustand des ISMS nachvollziehbar präsentieren können.

## Abkürzungsverzeichnis

| | |
|---|---|
| Eff | Effektivität |
| GQM | Goal Question Metric |
| IKT | Informations- und Kommunikationstechnologie |
| ISM | Informationssicherheitsmanagement |
| ISMS | Informationssicherheitsmanagementsystem |
| PDV | Prozessdatenverarbeitung |
| PGQM | Prozessorientierte Goal Question Metric |
| ZEG | Zielerfüllungsgrad |

## Literaturverzeichnis

BASILI, V. R., CALDIERA, G., ROMBACH, H. D. (1994): The Goal Question Metric Approach, Encyclopedia of Software Engineering, S. 528–532, John Wiley & Sons.

BASILI, V.R., WEISS, D.M. (1982): A Methodology for Collecting Valid Software Engineering Data, Technical Report, Naval Research Laboratory.

BUNDESNETZAGENTUR (2011): Smart Grid und Smart Market, Bundesnetzagentur.

DIN DEUTSCHES INSTITUT FÜR NORMUNG E. V. (2015): DIN ISO/IEC 27001:2015: Informationstechnologie – Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen.

DORAN, G. T. (1981): There's a S.M.A.R.T. way to write management's goals and objectives. Management Review, Volume 70, Issue 11, 1981, S. 35-36.

HAYDEN, L. (2010): IT Security Metrics - A Practical Framework for Measuring Security & Protecting Data.

DIN DEUTSCHES INSTITUT FÜR NORMUNG E.V. (2005): DIN EN ISO 9000:2005: Qualitätsmanagementsysteme - Grundlagen und Begriffe.

DIN DEUTSCHES INSTITUT FÜR NORMUNG E.V. (2008): DIN EN ISO 9001:2008: Qualitätsmanagementsysteme – Anforderungen.

DIN DEUTSCHES INSTITUT FÜR NORMUNG E.V. (2009): DIN EN ISO 9004:2009: Leiten und Lenken für den nachhaltigen Erfolg einer Organisation – Ein Qualitätsmanagementansatz.

ISO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION UND IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION (2014): ISO/IEC 27000:2014: Information technology – Security techniques – Information security management systems -- Overview and vocabulary.

ISO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION UND IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION (2013): ISO/IEC 27001:2013: Information technology -- Security techniques -- Information security management systems – Requirements.

ISO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION UND IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION (2013): ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security controls.

SO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION UND IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION (2009): ISO/IEC 27004:2009: Information technology — Security techniques — Information security management — Measurement.

ISO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION UND IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION (2013): ISO/IEC Directives, Part 1 Consolidated ISO Supplement — Procedures specific to ISO.

ISO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION UND IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION (2013): ISO/IEC TR 27019:2013: Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

OPEN GROUP (2011): Open Information Security Management Maturity Model (O-ISM3).

SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON UNIVERSITY (2010): CMMI® for Development, Version 1.3, CMU/SEI-2010-TR-033.

SCHMELZER, H.J., SESSELMANN, W. (2013): Geschäftsprozessmanagement in der Praxis, 8. Auflage.
VDE – VERBAND DER ELEKTROTECHNIK ELEKTRONIK INFORMATIONSTECHNIK E.V. (2014): VDE-Positionspapier Smart Grid Security - Energieinformationsnetze und -systeme, Frankfurt/Main 2014

## Tabellen- und Abbildungsverzeichnis

### Abbildungen



### Tabellen

## Working Papers des Institute of Management Berlin an der Hochschule für Wirtschaft und Recht Berlin

1 Bruche, Gert/ Pfeiffer, Bernd: Herlitz (A) – Vom Großhändler zum PBS-Konzern – Fallstudie, Oktober 1998.
2 Löser, Jens: Das globale Geschäftsfeld „Elektrische Haushaltsgroßgeräte“ Ende der 90er Jahre – Fallstudie, Oktober 1998.
3 Lehmann, Lutz Lars: Deregulation and Human Resource Management in Britain and Germany – Illustrated with Coca-Cola Bottling Companies in Both Countries, March 1999.
4 Bruche, Gert: Herlitz (B) - Strategische Neuorientierung in der Krise - Fallstudie, April 1999.
5 Herr, Hansjörg/ Tober, Silke: Pathways to Capitalism - Explaining the Difference in the Economic Development of the Visegrad States, the States of the Former Soviet Union and China, October 1999.
6 Bruche, Gert: Strategic Thinking and Strategy Analysis in Business - A Survey on the Major Lines of Thought and on the State of the Art, October 1999, 28 pages.
7 Sommer, Albrecht: Die internationale Rolle des Euro, Dezember 1999, 31 pages.
8 Haller, Sabine: Entwicklung von Dienstleistungen - Service Engineering und Service Design, Januar 2000.
9 Stock, Detlev: Eignet sich das Kurs-Gewinn-Verhältnis als Indikator für zukünftige Aktienkursveränderungen?, März 2000.
10 Lau, Raymond W.K.: China’s Privatization, June 2000.
11 Breslin, Shaun: Growth at the Expense of Development? Chinese Trade and Export-Led Growth Reconsidered, July 2000, 30 pages.
12 Michel, Andreas Dirk: Market Conditions for Electronic Commerce in the People’s Republic of China and Implications for Foreign Investment, July 2000, 39 pages.
13 Bruche, Gert: Corporate Strategy, Relatedness and Diversification, September 2000, 34 pages.
14 Cao Tingui: The People's Bank of China and its Monetary Policy, October 2001, 21 pages.
15 Herr, Hansjörg: Wages, Employment and Prices. An Analysis of the Relationship Between Wage Level, Wage Structure, Minimum Wages and Employment and Prices, June 2002, 60 pages.
16 Herr, Hansjörg/ Priewe, Jan (eds.): Current Issues of China’s Economic Policies and Related International Experiences – The Wuhan Conference 2002 - , February 2003, 180 pages.
17 Herr, Hansjörg/ Priewe, Jan: The Macroeconomic Framework of Poverty Reduction An Assessment of the IMF/World Bank Strategy, February 2003, 69 pages.
18 Wenhao, Li: Currency Competition between EURO and US-Dollar, June 2004, 18 pages.
19 Kramarek, Maciej: Spezifische Funktionen des Leasings in der Transformationsperiode, Juni 2004, 32 pages.
20 Godefroid, Peter: Analyse von Multimedia-Lern/Lehrumgebungen im Fach Marketing im englischsprachigen Bereich – inhaltlicher Vergleich und Prüfung der Einsatzfähigkeit an deutschen Hochschulen, September 2004, 48 pages.
21 Kramarek, Maciej: Die Attraktivität des Leasings am Beispiel polnischer Regelungen der Transformationsperiode, April 2005, 33 pages.
22 Pan, Liu/Tao, Xie: The Monetary Policy Transmission in China – „Credit Channel” and its Limitations.
23 Hongjiang, Zhao/ Wenxu, Wu/Xuehua, Chen: What Factors Affect Small and Medium-sized Enterprise’s Ability to Borrow from Bank: Evidence from Chengdu City, Capital of South-western China’s Sichuan Province, May 2005, 23 pages.
24 Fritsche, Ulrich: Ergebnisse der ökonometrischen Untersuchung zum Forschungsprojekt Wirtschaftspolitische Regime westlicher Industrienationen, March 2006, 210 pages.
25 Körner, Marita: Constitutional and Legal Framework of Gender Justice in Germany, November 2006, 14 pages.
26 Tomfort, André: The Role of the European Union for the Financial Integration of Eastern Europe, December 2006, 20 pages.
27 Gash, Vanessa/ Mertens, Antje/Gordo, Laura Romeu: Are Fixed-Term Job Bad for Your Health? A Comparison between Western Germany and Spain, March 2007, 29 pages.
28 Kamp, Vanessa/ Niemeier, Hans-Martin/Müller, Jürgen: Can we Learn From Benchmarking Studies of Airports and Where do we Want to go From Here? April 2007, 43 pages.
29 Brand, Frank: Ökonomische Fragestellungen mit vielen Einflussgrößen als Netzwerke. April 2007, 28 pages.
30 Venohr, Bernd/ Klaus E. Meyer: The German Miracle Keeps Running: How Germany’s Hidden Champions Stay Ahead in the Global Economy. May 2007, 31 pages.
31 Tomenendal, Matthias: The Consultant-Client Interface - A Theoretical Introduction to the Hot Spot of Management Consulting. August 2007, 17 pages.
32 Zenglein, Max J.: US Wage Determination System. September 2007, 30 pages.
33 Figeac, Alexis: Socially Responsible Investment und umweltorientiertes Venture Capital. December 2007, 45 pages.
34 Gleißner, Harald A.: Post-Merger Integration in der Logistik - Vom Erfolg und Misserfolg bei der Zusammenführung von Logistikeinheiten in der Praxis. March 2008, 27 pages.
35 Bürkner, Fatiah: Effektivitätssteigerung im gemeinnützigen Sektor am Beispiel einer regionalen ‚Allianz für Tanz in Schulen’. April 2008, 29 pages.

36 Körner, Marita: Grenzüberschreitende Arbeitsverhätnisse - Grundlinien des deutschen Internationalen Privatrechts für Arbeitsverträge. April 2008, 22 pages.
37 Pan, Liu/ Junbo, Zhu: The Management of China's Huge Foreign Reserve and ist Currency Composition. April 2008, 22 pages.
38 Rogall, Holger: Essentiales für eine nachhaltige Energie- und Klimaschutzpolitik. May 2008, 46 pages.
39 Maeser, Paul P.: Mikrofinanzierungen - Chancen für die Entwicklungspolitik und Rahmenbedingungen für einen effizienten Einsatz. May 2008, 33 pages.
40 Pohland, Sven/ Hüther, Frank/ Badde, Joachim: Flexibilisierung von Geschäftsprozessen in der Praxis: Case Study „Westfleisch eG - Einführung einer Service-orientierten Architektur (SOA). June 2008, 33 pages.
41 Rüggeberg, Harald/ Burmeister, Kjell: Innovationsprozesse in kleinen und mittleren Unternehmen. June 2008, 37 pages.
42 Domke, Nicole/ Stehr, Melanie: Ignorieren oder vorbereiten? Schutz vor Antitrust Verstößen durch Compliance"-Programme. June 2008, 25 pages.
43 Ripsas, Sven/ Zumholz, Holger/ Kolata, Christian: Der Businessplan als Instrument der Gründungsplanung - Möglichkeiten und Grenzen. December 2008, 34 pages.
44 Jarosch, Helmut: Optimierung des Zusammenwirkens maschineller und intellektueller Spezialisten. January 2009, 35 pages.
45 Kreutzer, Ralf T./ Salomon, Stefanie: Internal Branding: Mitarbeiter zu Markenbotschaftern machen – dargestellt am Beispiel von DHL. February 2009, 54 pages.
46 Gawron, Thomas: Formen der überörtlichen Kooperation zur Steuerung der Ansiedlung und Erweiterung von großflächigen Einzelhandelsvorhaben. April 2009, 43 pages.
47 Schuchert-Güler, Pakize: Aufgaben und Anforderungen im persönlichen Verkauf: Ergebnisse einer Stellenanzeigenanalyse. April 2009, 33 pages.
48 Felden, Birgit/ Zumholz, Holger: Managementlehre für Familienunternehmen – Bestandsaufnahme der Forschungs- und Lehraktivitäten im deutschsprachigen Raum. July 2009, 23 pages.
49 Meyer, Susanne: Online-Auktionen und Verbraucherschutzrecht – ein Rechtsgebiet in Bewegung. Zugleich ein Beitrag zu Voraussetzungen und Rechtsfolgen des Widerrufsrechts bei Internetauktionen. December 2009, 29 pages.
50 Kreutzer, Ralf T.: Konzepte und Instrumente des B-to-B-Dialog-Marketings. December 2009, 40 pages.
51 Rüggeberg, Harald: Innovationswiderstände bei der Akzeptanz hochgradiger Innovationen aus kleinen und mittleren Unternehmen. December 2009, 31 pages.
52 Kreutzer, Ralf T.: Aufbau einer kundenorientierten Unternehmenskultur. December 2009, 59 pages.
53 Rogall, Holger/ Oebels, Kerstin: Von der Traditionellen zur Nachhaltigen Ökonomie, June 2010, 28 pages.
54 Weimann, Andrea: Nutzung von Mitarbeiterpotenzialen durch Arbeitszeitflexibilisierung – Entwicklung eines optimierten Arbeitszeitmodells für eine Abteilung im Einzelhandel, June 2010, 35 pages.
55 Bruche, Gert: Tata Motor's Transformational Resource Acquisition Path – A Case Study of Latecomer Catch-up in a Business Group Context, October 2010, 28 pages.
56 Frintrop, Philipp/ Gruber, Thomas: Working Capital Management in der wertorientierten Unternehmenssteuerung bei Siemens Transformers, November 2010, 35 pages.
57 Tolksdorf, Michael: Weltfinanzkrise: Zur Rolle der Banken, Notenbanken und „innovativer Finanzprodukte", November 2010, 20 pages.
58 Kreutzer, Ralf T./ Hinz ,Jule: Möglichkeiten und Grenzen von Social Media Marketing, December 2010, 44 pages.
59 Weyer,Birgit: Perspectives on Optimism within the Context of Project Management: A Call for Multilevel Research, January 2011, 30 pages.
60 Bustamante, Silke: Localization vs. Standardization: Global approaches to CSR Management in multinational companies, March 2011, 29 pages.
61 Faltin, Günter/Ripsas, Sven: Das Gestalten von Geschäftsmodellen als Kern des Entrepreneurship, April 2010, 22 pages.
62 Baumgarth, Carsten/ Binckebanck, Lars: CSR-Markenmanagement – Markenmodell und Best-Practice-Fälle am Beispiel der Bau- und Immobilienwirtschaft, September 2011, 46 pages
63 Lemke, Claudia: Entwurf eines Modells zur serviceorientierten Gestaltung von kleinen IT-Organisationen in Forschungseinrichtungen Theoretische Überlegungen und methodische Konzeption als erste Ergebnisse eines Forschungsprojektes an der HWR Berlin, October 2011, 43 pages
64 Greiwe, Joris/ Schönbohm, Avo: A KPI based study on the scope and quality of sustainability reporting by the DAX 30 companies, November 2011, 31 pages
65 Lemke, Claudia: Auszug aus der Modellierung des IT-Dienstleistungsmodells „proITS" am Beispiel der Struktur von Forschungseinrichtungen und deren IT-Service – Erkenntnisse aus einem Forschungsprojekt an der HWR Berlin, February 2012, 46 pages.
66 Grothe, Anja/ Marke, Nico: Nachhaltiges Wirtschaften in Berliner Betrieben – Neue Formen des Wissenstransfers zwischen Hochschule und Unternehmen, March 2012, 40 pages.
67 Meyer, Susanne/ Fredrich, Jan: Rechtsgrundlagen einer Pflicht zur Einrichtung einer Complance-Organisation, May 2012, 19 pages.
68 Schönbohm, Avo/ Hofmann, Ulrike: Comprehensive Sustainability Reporting – A long road to go for German TecDax 30 companies, June 2012, 23 pages.
69 Baumgarth, Carsten/ Kastner, Olga Louisa: Pop-up-Stores im Modebereich: Erfolgsfaktoren einer vergänglichen Form der Kundeninspiration, July 2012, 33 pages.

70 Bowen, Harry P./ Pédussel Wu, Jennifer: Immigrant Specificity and the Relationship between Trade and Immigration: Theory and Evidence, October 2012, 32 pages.
71 Tomenendal, Matthias: Theorien der Beratung – Grundlegende Ansätze zur Bewertung von Unternehmensberatungsleistungen, December 2012, 35 pages.
72 Schönbohm, Avo: Performance Measurement and Management with Financial Ratios – the BASF SE Case, March 2013, 26 pages.
73 Olischer, Florian/ Dörrenbächer, Christoph: Concession Bargaining in the Airline Industry: Ryanair's Policy of Route Relocation and Withdrawal, April 2013, 26 pages.
74 Dörrenbächer, Christoph/ Gammelgaard, Jens/ McDonald, Frank, Stephan, Andreas/ Tüselmann, Heinz: Staffing Foreign Subsidiaries with Parent Country Nationals or Host Country National? Insights from European Subsidiaries, September 2013, 27 pages.
75 Aschfalk-Evertz, Agnes/ Rüttler Oliver: Goodwill Impairment Testing according to IFRS in the United Kingdom - An empirical analysis of the discount rates used by the thirty largest FTSE 100 companies, November 2013, 28 pages.
76 Stockklauser, Stephanie/ Tomenendal, Matthias: The Value of Political Consulting – A Segmentation of Services and Evaluation Tools, December 2013, 40 pages.
77 Rosentreter, Sandra/ Singh, Penny/ Schönbohm, Avo: Research Output of Management Accounting Academics at Universities of Applied Sciences in Germany and Universities of Technology in South Africa - A Comparative Study of Input Determinants, December 2013, 33 pages.
78 Baumgarth, Carsten/Sandberg, Berit/Brunsen, Hendrik/Schirm, Alexander: Kunst-Unternehmens-Kooperationen (KUK) - Begriffsbestimmung, Typologie und potenzieller Nutzen, January 2014, 43 pages.
79 Tomenendal, Matthias/Lange, Hans Rüdiger: Cluster-Entwicklung in einem dreistufigen Modell: das Fallbeispiel des Berlin-Brandenburger Energietechnik-Clusters, June 2014, 31 pages.
80 Rhode, Alexander/ Schönbohm, Avo/ van Vliet, Jacobus: The Tactical Utilization of Cognitive Biases in Negotiations, June 2014, 28 pages.
81 Tomendal, Mathias/Bernhard, Martin G.: Die virtuelle Beratungsorganisation am Rand des Chaos – Wie ein kleines Unternehmen große Projekte durchführen kann, August 2014, 27 pages.
82 Fischer, Ingo/Kieler, Julia: Towards an Employer Brand – An Evidence-Based Approach to Develop an Employer Brand: A Case Study of a Berlin-Based Business Incubator in the Online and Mobile Gaming Industry, April 2015, 28 pages.

**Special Edition:**
Ben Hur, Shlomo: A Call to Responsible Leadership. Keynote Speech at the FHW Berlin MBA Graduation Ceremony 2006. November 24th, 2006, Berlin City Hall, April 2007, 13 pages.

Imprint

Series Editor
Head of IMB Institute of Management Berlin

ISSN
1869-8115

Print
HWR Berlin

Berlin June 2015

www.hwr-berlin.de