



*Information Systems
Audit and Control
Association*

Switzerland Chapter

**Revision
Healthcheck
Risikoanalyse
Sicherheitskonzept
Sicherheitshandbuch**

**CoP
COBIT
Marion
IT-Grundschutzhandbuch**

–

**vier Methoden
im Vergleich**

**Interessengruppe “Code of Practice”
– die Ergebnisse**

© 29.9.1998

© ISACA Switzerland Chapter

c/o Maher Kamal, CISA

Arthur Andersen AG

Binzmühlestr. 14, 8050 Zürich

Tel: 01 / 308 18 88

*Nachdruck mit Quellenangabe gestattet;
um ein Referenzexemplar an obige Adresse wird gebeten*

Beiträge:	Mitglieder der Interessengruppe "Code of Practice"
Layout und Gestaltung:	Peter R. Bitterli
Zeichnungen:	Rolf Kränzlin, 8050 Zürich
Abbildungen:	Mitglieder der Interessengruppe "Code of Practice"
	Kopien aus Originalunterlagen

Inhaltsverzeichnis

Die Interessengruppe “Code of Practice”	4
Ziele, Vorgehen, Teilnehmer	
Vorstellung von Methoden und Begriffen	5
Übersicht	
Der Code of Practice for Information Security Management (CoP)	7
Der Leitfaden zum Management der Informationssicherheit	
COBIT (Governance, Control and Audit for Information and Related Technology)	13
Der Standard für Sicherheit, Qualität und Ordnungsmässigkeit der Informationstechnologie	
Marion (Méthode d’Analyse des Risques Informatiques et d’Optimisation par Niveau)	19
Die Risikoanalysemethode mit Simulation und Sicherheitsplanung	
IT-Grundschutzhandbuch	23
Das Handbuch für sichere Anwendung der Informationstechnik	
Die Resultate der Umfrage	27
Ergebnisse einer bei allen Mitgliedern von SWISS-ISA durchgeführten Umfrage zum Methodenvergleich	

Die Interessengruppe "Code of Practice"



Während zweier Jahre trafen sich die Mitglieder der IG CoP in recht kurzen Abständen zu Kurzreferaten, Software-Demonstrationen und auch zu intensiven Diskussionen. Zudem arbeiteten sie in mehreren Untergruppen an den verschiedensten Teilthemen. Ausgangspunkt der recht heterogen zusammengesetzten Gruppe war das Thema "Grundschutz für Informationssicherheit" am Beispiel des CoP (mit vollem Namen "A Code of Practice for Information Security Management").

Die Ziele der IG waren:

- a) den CoP mit anderen Methoden zu vergleichen;
- b) die Anwendungsmöglichkeiten der verschiedenen Methoden kennenzulernen;
- c) Implementierungshilfen für derartige Projekte zu erarbeiten.

Die IG CoP hat verschiedene ähnliche Standards "angeschaut" und drei davon miteinander und mit dem CoP verglichen – so das Grundschutzhandbuch des BSI, COBIT von ISACA oder MARION von PSI. Sehr wertvoll war hier die extensive Erfahrung aller Mitglieder der Interessengruppe mit den oben erwähnten Methoden resp. in den Anwendungsgebieten "Erstellung eines Sicherheitskonzeptes oder eines Sicherheitshandbuchs" oder "Durchführung einer Sicherheitsanalyse resp. einer Revision".

Das Thema schien auch andere zu interessieren: Immer wieder erhielt die IG Anfragen, ob man nicht der Gruppe beitreten könnte. Da man aber bereits schon sehr lange und intensiv miteinander zusammengearbeitet hatte, wollte man das gute Funktionieren der Gruppe nicht gefährden. Die Interessenten mussten auf später vertröstet werden.

Mit der Zeit wuchs das Interesse der IG-Mitglieder, die Erfahrungen anderer in ihre Diskussionen einfließen zu lassen. So wurden für eine Umfrage zwei Fragebogen entwickelt, an alle Mitglieder von SWISS-ISA (ISACA Switzerland Chapter, Clusis und SI Security) versandt und die zurückgeschickten Exemplare ausgewertet. Die Ergebnisse bestätigten mehrheitlich die eigenen Erfahrungen, doch in einigen Fällen kam man doch zu überraschenden Erkenntnissen.

Die Leistung der IG CoP soll und kann man an ihren Ergebnissen messen – doch sind diese nur ein Teil dessen, was jeder einzelne Teilnehmer in die Gruppe eingebracht hat. Der offene Informationsfluss, die gute Zusammenarbeit an den Sitzungen und auch in den Teilgruppen sowie nicht zuletzt die persönlichen Kontakte waren für alle IG-Mitglieder wertvoll. Das Mitmachen in dieser Interessengruppe hat sich gelohnt!

Die Teilnehmer der IG in alphabetischer Reihenfolge:

Peter R. Bitterli, Bitterli Consulting AG

Ulrich Brügger, IBM

Michele Ferretti, Credit Suisse Group

Nils O. Gehrig, Winterthur-Versicherungen

Rolph Haefelfinger, PricewaterhouseCoopers

André Mooser, Migros-Genossenschafts-Bund

Felix Widmer, DCB Data Center Brütisellen AG

Vorstellung von Methoden und Begriffen

Die vier miteinander verglichenen Methoden

Code of Practice - CoP (British Standards Institution)

Der CoP ist eine praxisorientierte Festlegung der Mindestanforderungen im IT-Sicherheitsbereich. Die Themenbreite umfasst die Bereiche organisatorische, physische und logische Sicherheit sowie Anwendungsentwicklung und -unterhalt, Notfallvorsorge und Einhaltung/Überprüfung der Sicherheit. Die Thementiefe umfasst rund 110 allgemein anerkannte Sicherheitsanforderungen (Baseline Approach resp. Grundschutz). Mit dem Instrument der Key Controls (Schlüsselanforderungen) werden zusätzliche Prioritäten gesetzt und ein Einstieg in die Materie erleichtert. Der CoP hat den Status eines Britischen Standards (BS7799: 1995).

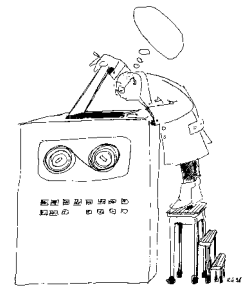
COBIT (Governance, Control and Audit for Information and Related Technology)

COBIT ist ein Framework, bestehend aus 34 zentralen Kontrollprozessen, welche die Abhängigkeit der Geschäftsprozesse von Informationen und (IT-) Ressourcen darstellen. Erst wenn Daten, Anwendungen, Anlagen, die Technologie und das Personal richtig "organisiert" sind, werden die Geschäftsprozesse die Anforderungen an Effektivität, Effizienz, Vertraulichkeit, Integrität, Verfügbarkeit, Compliance und Zuverlässigkeit erfüllen. Werden die rund 300 in COBIT enthaltenen Kontrollziele konsequent umgesetzt, kann eine geordnete Planung, Beschaffung und Überwachung aller eingesetzten IT-Ressourcen erreicht werden. COBIT ist 1996 von der ISACA erstmals und 1998 in einer aktualisierten Version veröffentlicht worden.

Marion

Marion (Méthode d'Analyse des Risques Informatiques et d'Optimisation par Niveau) ist eine Applikation zur Beurteilung der Informationssicherheit und basiert auf einer gleichnamigen Methode, welche von CLUSIF 1989 publiziert wurde. Eine Untersuchung mit Marion läuft in drei Phasen ab. Zuerst werden mit strukturierten Interviews und vorgegebenen Risikoszenarien diejenigen Risiken identifiziert, welche die Fortführung der Geschäftstätigkeit beeinträchtigen könnten. Danach werden 27 Bereiche der Informationssicherheit anhand eines jährlich angepassten Fragebogens bewertet und graphisch dargestellt. Zuletzt werden aus einer Erfahrungsdatenbank standardisierte Massnahmen vorgeschlagen. Diese werden in Form von funktionalen Anforderungen zusammen mit möglichen Implementationsvorschlägen dargestellt. Zusätzlich werden Sachkosten und personelle Aufwendungen als Schätzwerte berechnet.

...



IT-Grundschatzhandbuch 1997 (BSI, Bonn)

Das IT-Grundschatzhandbuch ist eine strukturierte Sammlung von Massnahmen aus den Bereichen Infrastruktur, Organisation, Personal, Hard- und Software, Kommunikation und Notfallvorsorge. Das regelmässig aktualisierte IT-Grundschatzhandbuch ist als Baukasten konzipiert. Damit wird eine modulare Anwendung erleichtert. Für jeden Bereich sind dabei die potentiellen Gefährdungen und mögliche Schutzmassnahmen aufgeführt. Einzelne Themen sind sehr detailliert dargestellt und können direkt übernommen werden. Generell ist der konzeptionelle Teil wenig ausgeprägt. Die Anwendung des Handbuches und die zu Grunde liegende Methodik (Baseline Approach resp. Grundschatz) ermöglichen einen schnellen Einstieg. Das IT-Grundschatzhandbuch enthält Fragebogen für die IT-Grundschatzerhebung.

Wichtige Begriffe

Es hat sich verschiedentlich gezeigt, dass auch Experten unter einem bestimmten Begriff nicht immer das Gleiche verstehen. Zum besseren Verständnis der nachfolgenden Kurzberichte drucken wir Ihnen in alphabetischer Reihenfolge "unsere" Version der fünf zentralen Anwendungen von solchen Methoden ab:

Healthcheck (Sicherheits-Benchmarking)

Rasch durchführbare Standortbestimmung bezüglich der Informationssicherheit.

Revision

Unabhängiger, neutraler Vergleich zwischen dem tatsächlichen und dem vorgegebenen Zustand (Soll/Ist-Vergleich) eines Regelwerks hinsichtlich seiner Zweckeignung und/oder Einhaltung.

Risikoanalyse

Methodische Ermittlung aller Risiken eines Systems durch Abschätzung der Eintretenswahrscheinlichkeit eines schädigenden Ereignisses und des damit verbundenen Schadensausmasses.

Sicherheitshandbuch

Nachvollziehbare Festlegung bzw. Umsetzung der im Sicherheitskonzept festgehaltenen Anforderungen in konkrete Massnahmen.

Sicherheitskonzept

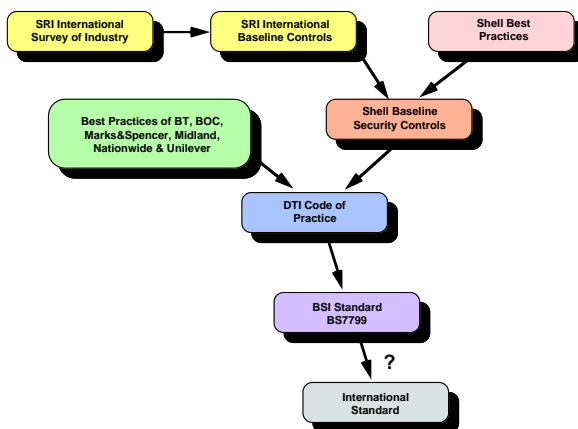
Systematische Festlegung der konzeptionellen Sicherheitsanforderungen und dem Vorgehen zu ihrer Umsetzung in Massnahmen.

Der “Code of Practice for Information Security Management (CoP)”



1. Geschichte

Der *Code of Practice for Information Security Management (CoP)* entstand aus dem Bedürfnis von Handel und Industrie nach einfach einsetzbaren Sicherheitsstandards. Hauptziel war, eine gemeinsame Basis zu erstellen für Unternehmen, die eine effektive Sicherheitsorganisation entwickeln, implementieren und messen wollen.



Basierend auf den Shell Baseline Security Controls wurde der Code of Practice unter der Leitung des Department of Trade and Industry (UK) und mit Hilfe einer Gruppe von führenden Unternehmen und Organisationen erarbeitet und im September 1993 offiziell verabschiedet. Zwei Jahre später erhielt der CoP den offiziellen Status eines Britischen Standards (BS7799), was einem Unternehmen dort ermöglicht, sich entsprechend zu zertifizieren.

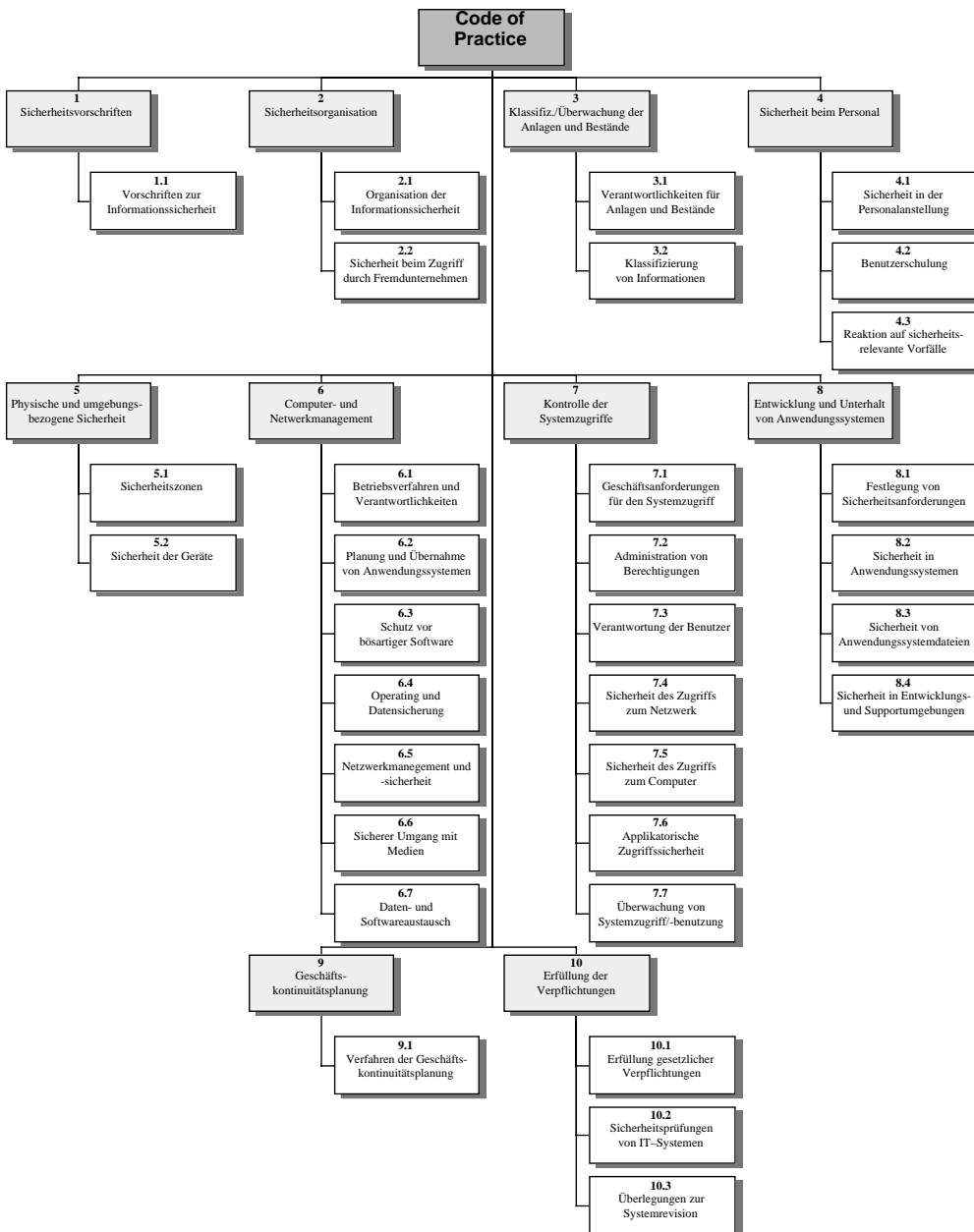
2. Vorstellung der Methode

Der Code of Practice enthält eine Sammlung von rund 110 allgemein anerkannten Sicherheitsanforderungen, die grundsätzlich und für jedes Unternehmen gültig sind – sogenannte *Baseline Controls* oder *Grundschutz-Massnahmen*. Die klare Struktur des CoP (zehn Hauptkapitel, die ihrerseits in mehrere themenspezifische Unterkapitel aufgeteilt sind) ermöglicht es dem Leser, im doch recht komplexen Themenkreis “Sicherheit” die Übersicht zu bewahren.

Die zehn Hauptkapitel enthalten (in Stichwörtern):

1. *Sicherheitsvorschriften*: Schriftlich festgehaltene Direktiven des Managements
2. *Sicherheitsorganisation*: Sicherheitsausschuss, Koordination von Sicherheitsbelangen, Verantwortlichkeiten, Verträge mit Externen
3. *Klassifizierung und Überwachung der Anlagen und Bestände*: Klassifizierungsrichtlinien, verantwortliche Eigentümer für Daten und Prozesse
4. *Sicherheit beim Personal*: Stellenbeschreibung, Rekrutierung, Vertraulichkeitsvereinbarung, Sensibilisierung, korrekte Reaktionen, Disziplinarmaßnahmen
5. *Physische und umgebungsbezogene Sicherheit*: Sicherheitszonen, Zutrittsregelungen, Sicherheit im Informatikbereich, Lieferanten, “Clear Desk”-Politik
6. *Computer- und Netzwerkmanagement*: Dokumentation von Abläufen/Verfahren, Funktionentrennung, Operating, Datenaustausch, Umgang mit Computermedien

7. *Kontrolle der Systemzugriffe*: Definition und Administration von Berechtigungen, Sicherheit von Netzwerk- und Rechnerzugriff, Überwachung der Zugriffe
8. *Entwicklung und Unterhalt von Anwendungssystemen*: Festlegung von Sicherheitsanforderungen, Entwicklungsstandards, Qualitätssicherung
9. *Geschäftskontinuitätsplanung*: Notfall-Organisation, Notfallkonzept, regelmäßige Tests und gesicherte Nachführung des Plans
10. *Erfüllung der Verpflichtungen*: Erfüllung der gesetzlichen und vertraglichen Verpflichtungen (Urheberrecht, Aufbewahrungsvorschriften, Datenschutz), Prüfung der Sicherheit



Der Code of Practice verzichtet auf allzu theoretische Überlegungen – er konzentriert sich darauf zu vermitteln, welche *konkreten* Schritte getroffen werden müssen, um die Risiken im Bereich der Informationssicherheit grundsätzlich zu verringern. Mit diesem pragmatischen Vorgehen lassen sich die erheblichen Kosten für detaillierte Risikoanalysen einsparen, mit denen sonst die zu realisierenden Sicherheitsmassnahmen ermittelt werden.

3. Hersteller/Lieferant

Der Code of Practice for Information Security Management (CoP) wurde unter der Schirmherrschaft des Department of Trade and Industry (UK) von mehreren Unternehmen gemeinsam entwickelt. Erhältlich ist er bei der Schweizer Normenvereinigung in Zürich.

Bezugsquelle

BS7799: A Code of Practice for Information Security Management, 1995, ISBN 0 580 23642 0, und dessen deutschsprachige Übersetzung "Leitfaden zum Management von Informationssicherheit" sind erhältlich bei der Schweizerischen Normenvereinigung, Tel. 01 254 54 54 für ca. Fr. 150 resp. Fr. 250.

4. Hauptanwendung: Erstellung eines Sicherheitskonzeptes

Der Code of Practice dient in der vorgestellten Form in erster Linie als Muster eines unternehmensinternen Sicherheitsstandards, was auch unsere Umfrage bestätigte. Basierend auf dem CoP lässt sich relativ einfach ein konsistentes Sicherheitskonzept erstellen, das die übergeordneten 109 Sicherheitsanforderungen sowie die rund 600 bis 800 verschiedenen Massnahmenpakete zu ihrer Abdeckung enthält. Die notwendigen Massnahmen lassen sich im Prinzip dem CoP entnehmen, doch ist der Detaillierungsgrad des Standards nicht in allen Belangen einheitlich. Geübte Personen benötigen für die genaue Formulierung der Massnahmen, insbesondere für ihre Gruppierung zu zusammengehörigen Massnahmenpaketen, etwa eine Woche – für erstmalige Anwender dürfte sich dieser Aufwand auf ein Mehrfaches erhöhen.

Die dem Code of Practice entnommenen Massnahmen sind in der Regel allgemein gültig (es handelt sich beim CoP ja um Grundsutzmassnahmen), doch dürfte die konkrete Ausgestaltung von der Art und Grösse des Unternehmens abhängen. Da der Code of Practice "nur" den Grundsutz regelt, müssen unter Umständen zusätzliche unternehmensspezifische Inhalte aufgenommen werden.

Zur Abdeckung der geschäftsspezifischen Risiken enthält der Code of Practice praktisch keine Anforderungen. Aufgeführt hingegen ist das Ziel, dass applikationsabhängige Sicherheitsanforderungen in einer der ersten Projektphasen systematisch ermittelt werden müssen, und dass alle notwendigen Massnahmen vor der Inbetriebnahme der Anwendung implementiert sein müssen.

5. Stärken und Schwächen der Methode

Die Stärken des Code of Practice aus Optik der Autoren liegen bei der Umsetzbarkeit, der Anpassbarkeit sowie bei der Zertifizierbarkeit und Standardisierung: Der Code of Practice ist sehr praxis- und massnahmenbezogen und lässt sich relativ gut in konkrete Massnahmen umsetzen. Dank seiner übersichtlichen Struktur und vor allem auch bei Einsatz der Software CoP-iT lässt sich der Code of Practice mit einem bescheidenen Aufwand an die Gegebenheiten des Unternehmens anpassen, wobei aber die geschäftsspezifischen Sicherheitsanforderungen nicht "enthalten" sind.

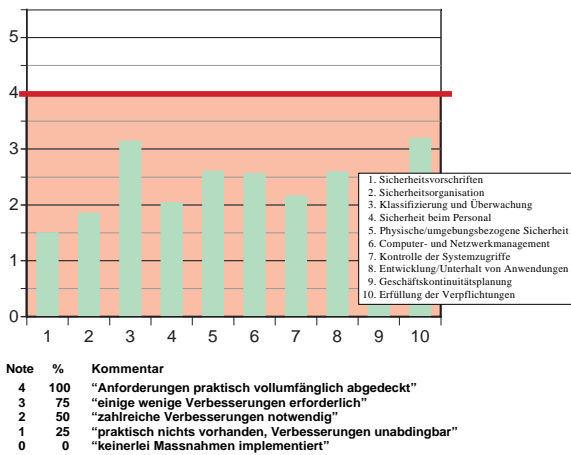
In Europa ist zudem die Tatsache der Standardisierung relativ wichtig: der Code of Practice findet in praktisch allen Branchen (bis hin zu Versicherungen und Banken)

breite Anerkennung. Einziger Wermutstropfen ist hier, dass USA-dominierte Konzerne USA-Standards den europäischen Standards vorzuziehen scheinen.

Letztlich ist die Wirtschaftlichkeit relativ gut: Mit einem bescheidenen internen und allenfalls externen Aufwand lässt sich ein qualitativ befriedigendes Sicherheitskonzept erstellen oder ein Healthcheck durchführen.

Die Resultate der Umfrage zeigen auf, dass auch die Unabhängigkeit des "Herausgebers" besonders geschätzt wird. Bemängelt wird allgemein die Resultatdarstellung, die jedoch mit relativ einfachen Tricks wesentlich verbessert werden kann (siehe Anwendungstips). Kritisiert wurde auch, dass der Code of Practice seit seiner Veröffentlichung als BS7799 nicht mehr verändert wurde. Hier ist der Hersteller daran, für 1999 eine aktualisierte Version vorzubereiten.

6. Denkbare andere Einsatzgebiete



Gut geeignet ist der Code of Practice für Risikoanalysen resp. für Health Checks (Sicherheitsbenchmarking), was auch in unserer Umfrage bestätigt wurde. Mit Hilfe der nachfolgend vorgestellten Software oder auch mit einer relativ simplen Checkliste in einem Tabellenkalkulationsprogramm kann auf der Basis der 10 Haupt- oder 32 Unterkapitel graphisch dargestellt werden, wo die grössten Risiken liegen resp. wie gross der Handlungsbedarf für eine Sanierung ist.

Wird der Code of Practice für Risikoanalysen eingesetzt, so muss man sich dessen bewusst sein, dass der CoP als Grundschutz-Standard keinerlei unternehmensspezifischen Risiken misst, sondern nur die Differenz zwischen einem Katalog von Standardmassnahmen und den bereits implementierten Massnahmen aufzeigen kann. Ob effektiv ein Risiko vorliegt, müsste gegebenenfalls noch zusätzlich abgeklärt werden.

7. Nicht geeignet für ...

Weniger geeignet ist der Code of Practice für die Erstellung eines Sicherheitshandbuchs: Auch wenn in einigen Fällen konkrete Massnahmen vorgestellt werden, fehlt in der Regel der dafür benötigte Detaillierungsgrad. Hier erstaunt, dass gemäss unserer Umfrage immerhin über ein Fünftel der Einsender den CoP gerade für diesen Zweck einsetzen. Es gibt unseres Erachtens zwei mögliche Gründe für diese Abweichung: Entweder sind die so erstellten Sicherheitshandbücher nicht allzu detailliert oder die Vorgaben des Code of Practice werden mit eigenen Praxiserfahrungen oder durch Einbezug des Grundschutzhandbuchs des BSI in Deutschland weiter detailliert.

8. Software-Unterstützung

Sehr günstig ist die Software CoP-iT von SMH in London: Für rund 700 Franken erhalten Sie die Software (Windows 3.1) sowie ein offizielles Exemplar des Standards BS7799. Die Software kommt auf drei Disketten, lässt sich meist problemlos installieren und ist sofort einsetzbar. Die

Benutzeroberfläche hält sich strikt an die Struktur des CoP, so dass die Orientierung leicht fällt. Neben der CoP-Struktur mit 10 Haupt- und 32 Unterkapiteln mit den insgesamt 109 Sicherheitsanforderungen enthält die Software auf der untersten Stufe für jeden dieser 109 Teilbereiche bis zu einem Dutzend Fragen zu Detailmassnahmen, deren Abdeckungsgrad jeweils mit 0, 25, 50, 75 und 100% bewertet werden muss.

Themen, die in einem Unternehmen keine Rolle spielen (z.B. falls die Firma keinerlei externen Netzanschlüsse hat), können einfach unterdrückt werden, so dass weder Fragen dazu gestellt werden noch diese Themen dann in der Bewertung mit irgendwelchen fiktiven Werten ausgefüllt werden müssen. Im weiteren ist beim Ausfüllen sehr gut ersichtlich, welche Teilfragen noch offen sind. Ist die Bewertung abgeschlossen, können auf Knopfdruck verschiedene Standard-Auswertungen erstellt und Berichte in die üblichen Textverarbeitungsprogramme exportiert werden. Wertvoll ist, dass bei jeder Frage der zugehörige Teil des Code of Practice angezeigt werden kann. Auf Wunsch kann man diesen auch komplett ausdrucken oder elektronisch weiterverarbeiten (unter Beachtung des Urheberrechts).

Einige andere Hersteller haben den CoP in ihre Werkzeuge integriert, so z.B. DDIS, Baseline Tool von Zbinden Infosec. Wir haben diese Produkte nicht angeschaut.

9. Ausblick: Erweiterungen, Ergänzungen, ...

Derzeit sind Bestrebungen im Gang, den Code of Practice als ISO-Norm zu etablieren, so dass man sich auch in anderen Ländern diesbezüglich zertifizieren lassen kann. Zugleich findet momentan eine Aktualisierung des Inhalts sowie eine Überarbeitung der Software CoP-iT statt (neue Plattform Windows95, Windows NT noch offen).

10. Anwendungstips

Es lohnt sich, den Code of Practice nicht nur als Quelle für ein Sicherheitskonzept zu verwenden sondern damit vorgängig ein Health Check (Sicherheitsbenchmarking) durchzuführen. Der mehrfache Nutzen dieses Vorgehens ist: bessere Kenntnis des Inhalts bei der Projektgruppe wie auch bei den betroffenen Personen, Aufzeigen des Handlungsbedarfs und damit Prioritätensetzung für Implementierung von Massnahmen, Sensibilisierung des Managements (Budget!). Verwendet man den Code of Practice für Healthcheck oder Risikoanalysen, so sollte man die ermittelten Werte in ein Tabellenkalkulationsprogramm oder spezielle Grafiksoftware exportieren und dort eigene Rosettendiagramme generieren.

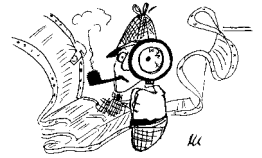
Bezugsquelle Software

SMH Associates plc, 5 Forest Court, Oaklands Park, Fishpond Road, Wokingham, Berks RG41 2QJ, Tel: (0118) 9362500, Fax: (0118) 9770764, E-Mail: help@smhplc.co.uk, Achtung: Demnächst soll ein neuer Release des CoP und auch der Software CoP-iT herauskommen.



Der Code of Practice – ein ganz spezieller Cop

COBIT (Governance, Control and Audit for Information and Related Technology)

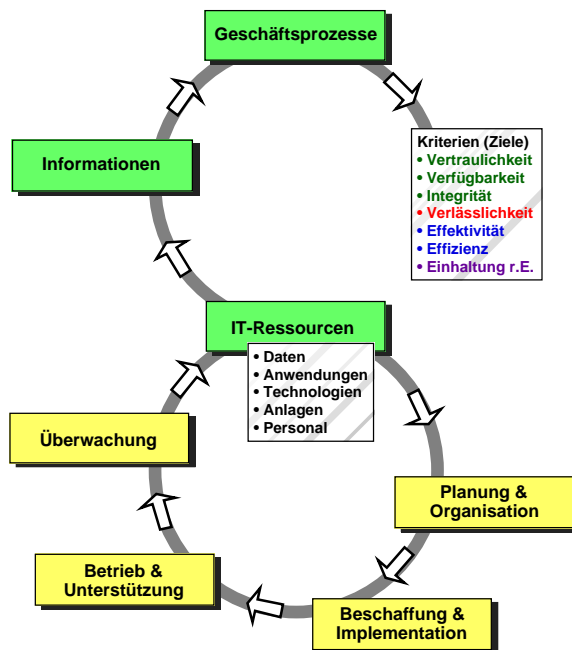


1. Geschichte

1992 kam das ISACA-Gremium, das sich mit der Überarbeitung der hauseigenen "Control Objectives for IT" beschäftigte, zum Schluss, dass diese nicht mehr den Bedürfnissen genügte. Auch andere verfügbare IT-Kontrollstandards wie der CoP des britischen DTI und das Security Handbook des amerikanischen NIST deckten nach Auffassung der ISACA nur einen Teil des IT-Kontrollspektrums ab, nämlich die Informationssicherheit. Es wurde ein Projekt gestartet zur Entwicklung eines umfassenden, mit den Geschäftskontroll-Modellen abgestimmten Standards für IT-Kontrolle.

Mehrere internationale Expertengruppen teilten sich in dieser Arbeit, welche zwei Jahre dauerte. Ende 1995 wurde als erstes Resultat das Framework publiziert, das ein IT-Kontrollmodell darstellt und die 32 übergeordneten IT-Prozesse enthält. 1996 wurden die 271 detaillierten Kontrollziele und die Audit Guidelines herausgegeben und unter den ISACA-Mitgliedern verbreitet (auf dieser Version basieren die Umfrageergebnisse zu COBIT). Im Mai 1998 erschien eine komplett überarbeitete und um einige wesentlichen Elemente erweiterte Version mit 34 IT-Prozessen und 300 Kontrollzielen.

2. Vorstellung der Methode

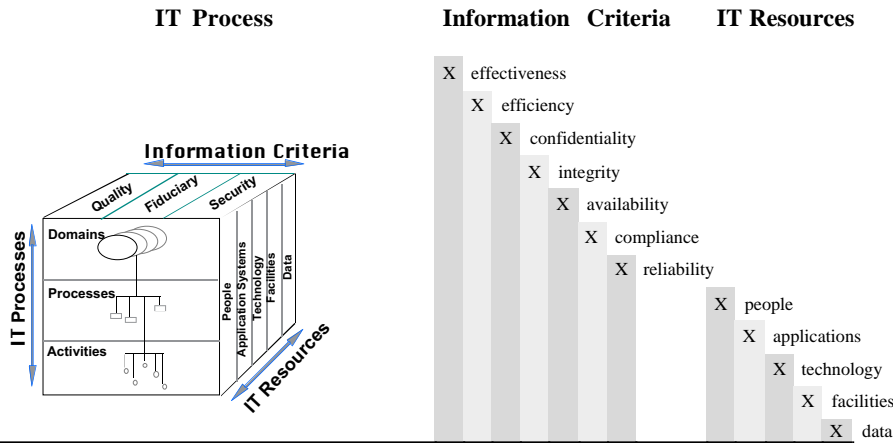


COBIT ist ein Standard für Kontrolle in der IT. Er beschreibt die Kontroll-Ziele, die in einer IT-Umgebung erreicht werden müssen, damit man von einer sicheren und ordnungsgemäßen Informationsverarbeitung sprechen kann.

Für die Formulierung der Kontrollziele werden sieben Arten von Geschäftsanforderungen berücksichtigt: die klassischen Sicherheitsanforderungen *Vertraulichkeit*, *Integrität* und *Verfügbarkeit*, weiter *Effektivität* (Wirksamkeit), *Effizienz* (Wirtschaftlichkeit), *Compliance* (Einhaltung rechtlicher Erfordernisse) und *Zuverlässigkeit* (Ordnungsmässigkeit bzgl. der Berichterstattung).

Die Struktur der Kontrollziele lehnt sich an ein prozessorientiertes Geschäftsmodell an. Dieses unterscheidet innerhalb der Informationstechnologie 34 zentrale IT-Prozesse, welche in den vier Domains *Planung & Organisation*, *Beschaffung & Implementation*, *Betrieb & Unterstützung*, *Überwachung* zusammengefasst werden.

Für jeden dieser Prozesse formuliert COBIT ein übergeordnetes Kontrollziel und zwischen 3 und 30 Detailziele. Die untenstehende Tabelle enthält alle IT-Prozesse und zeigt auf, welche der Geschäftsanforderungen durch die in jedem IT-Prozess definierten Kontrollziele abgedeckt werden und welche IT-Ressourcen davon in erster Linie betroffen sind.



IT Process	Information Criteria	IT Resources
PO1	effectiveness	people
PO2	efficiency	applications
PO3	confidentiality	technology
PO4	integrity	facilities
PO5	availability	data
PO6	compliance	
PO7	reliability	
PO8		
PO9		
PO10		
PO11		
AI1		
AI2		
AI3		
AI4		
AI5		
AI6		
DS1		
DS2		
DS3		
DS4		
DS5		
DS6		
DS7		
DS8		
DS9		
DS10		
DS11		
DS12		
DS13		
M1		
M2		
M3		
M4		

P = primary criteria √ = covers these resources
 S = secondary criteria

Bei der Anwendung von COBIT kann der Benutzer anhand dieser Tabelle bestimmen, welche IT-Prozesse für seine konkrete Situation relevant sind. Dabei hat er mehrere Ansatzmöglichkeiten zur Verfügung: er kann ganze Domains berücksichtigen (z.B. nur Überwachung) oder nur die Kontrollziele, die für die Erfüllung gewisser Geschäftsanforderungen (z.B. Vertraulichkeit, Integrität und Verfügbarkeit) nötig sind.

Das Produkt COBIT besteht aus 5 Bänden sowie drei Disketten und einer CD-ROM:

- "Executive Summary", welcher kurz den COBIT-Ansatz präsentiert
- "Framework", welcher die Philosophie und die Struktur des Werkes erklärt,
- "Control Objectives", welcher die 302 Kontrollziele enthält
- "Audit Guidelines", welcher für die 34 IT-Prozesse angibt, wie die richtige Implementation der Kontrollziele in einer IT-Umgebung geprüft werden kann.
- "Implementation Tool Set" mit einer Fülle von Information und Hilfsmitteln

3. Hersteller/Lieferant

Auftraggeber und Lieferant von COBIT ist die ISACA (Information Systems Audit and Control Association). Der Preis für das gesamte COBIT Package ist neu US\$ 195 (für ISACA-Mitglieder US\$ 100; als Upgrade

\$115 resp. \$75). Er kann bei der nebenstehenden Adresse bestellt werden. Die ersten drei Bände können als PDF gratis vom Internet heruntergeladen werden. Zusätzliche Informationen über das Produkt und über ISACA können im Internet eingesehen werden. Dort ist auch ein Bestellformular für COBIT zu finden.

Information Systems Audit and Control Association
135 S. LaSalle, Dept. 1055; Chicago, IL 60674-1055, USA
Phone: +847.253.1545, ext 401 Fax: +847.253.1443
Internet <http://www.isaca.org>

4. Hauptanwendung: Revision

COBIT wird hauptsächlich in der Revision verwendet, was in der Umfrage bestätigt wurde. Für das ganze Spektrum der IT-Aktivitäten offeriert COBIT dem IT-Revisor eine vollständige Palette von homogenen Kontrollzielen, welche er als Sollvorstellungen zur Beurteilung der Situation in der geprüften Einheit verwenden kann.

Die als Bestandteil des Produktes mitgelieferten (und in der zweiten Version nochmals erweiterten) Audit Guidelines erleichtern den Einsatz von COBIT. Basierend auf einem systematischen Vorgehensansatz zeigen diese Guidelines für jeden IT-Prozess auf, welche Schritte der Revisor bei seiner Prüfung durchlaufen muss – angefangen mit der Gewinnung von Informationen/Verständnis über das Prüfungsgebiet, über die Beurteilung der implementierten Kontrollen und der Einhaltung derselben bis zur Belegung und Einschätzung der vorhandenen Schwachstellen.

In COBIT sind die für jeden IT-Prozess zu erreichenden Kontrollziele bewusst auf einem relativ hohen Abstraktionsgrad formuliert. Entsprechend erfordert ein rein auf COBIT basierendes Prüfprogramm vom Revisor noch eine gute Dosis an Fachkompetenz, um die Angemessenheit der Implementation einer bestimmter Kontrolle zu beurteilen. Im Kapitel "Sicherstellen der Systemsicherheit" wird z.B. zum Thema "Authentisierung und Zugriffskontrolle" nur gefordert, dass "der logische Zugriff auf

und die Verwendung von Computer-Ressourcen durch die Implementation eines adäquaten Authentisierungsmechanismus, verbunden mit Zugriffsregeln, eingeschränkt wird". Zur Spezifikation dieser Mechanismen wird nur bemerkt, dass deren Effizienz gewährleistet werden muss. Wie das erreicht werden soll, z.B. wann anstelle eines einfachen Passwort-Systems ein starkes Authentisierungsverfahren verwendet werden soll, wird in COBIT nicht ausgeführt.

5. Stärken und Schwächen der Methode

Eine der Stärken von COBIT ist, dass er im Unterschied zu anderen bekannten Standards wie der CoP des britischen DTI oder das Security Handbook der amerikanischen NIST nicht durch eine nationale Behörde, sondern durch eine weltweit vertretene, unabhängige Organisation herausgegeben wurde. Er hat die besseren Voraussetzungen, um in allen Kontinenten akzeptiert zu werden - zumal er insgesamt 36 nationale wie internationale Standards "integriert".

Wegen des ungewohnten und eher abstrakten Ansatzes erfordert COBIT vom Benutzer einen nicht unbeträchtlichen Initialaufwand zum Verständnis der dahinterstehenden Logik. Man kann in diesem Sinne beim COBIT nicht von einem selbsterklärenden, anwenderfreundlichen Methode sprechen, doch hat sich die Situation mit der Informationsdatenbank auf der beigelegten CD-ROM wesentlich verbessert.

COBIT allein bietet nur wenig Unterstützung für die Darstellung der Analyseresultate. Einige nützliche Formulare sind auf der CD-ROM beigelegt, doch liefern diese "nur" tabellarisch und nicht grafisch dargestellte Ergebnisse. Es sind aber schon Produkte auf dem Markt, welche beigezogen werden können, um diese Lücke zu schliessen (siehe unter Software-Unterstützung).

6. Denkbare andere Einsatzgebiete

Ausser für Revisionen kann COBIT durch die Informatikabteilung selbst nach dem gleichen Muster für die Durchführung von Self-Assessments oder Healthcheck verwendet werden, wofür im Implementation Tool Set verschiedene Formulare und Denkansätze mitgeliefert werden.

COBIT wurde auch schon verschiedentlich für die Durchführung von Risikoanalysen eingesetzt. Man muss sich aber bei dieser Einsatzart bewusst sein, dass COBIT nicht zur Messung spezifischer Unternehmungsrisiken sondern nur zur Messung der Abweichung der implementierten Massnahmen von einem anerkannten Standard verwendet werden kann. Bei der Risikoquantifizierung kann COBIT wenig oder gar nicht helfen.

COBIT sollte sicher als Leitfaden bei der Implementierung des internen Kontrollsystems in der Unternehmungs-IT eingesetzt werden. Erfahrungen bei dieser Anwendung sind bei den Autoren noch wenige vorhanden.

7. Nicht geeignet für ...

Nicht geeignet ist COBIT für die Erstellung von Sicherheitshandbüchern. COBIT bleibt mit seinen Kontrollzielen auf der Ebene der Sollvorstellungen/Anforderungen an die Kontrolle. Ein Sicherheitshandbuch erfordert hingegen die detaillierte Beschreibung der zu implementierenden Sicherheitsmassnahmen und dies findet man in COBIT nicht.

8. Software-Unterstützung

Es sind uns momentan zwei Produkte bekannt, welche die Anwendung von COBIT in der Praxis unterstützen. Abzuklären ist, ob diese bereits an den neuen COBIT-Release angepasst wurden.

- "COBIT Advisor" von Methodware Limited in Wellington, New Zealand, erlaubt dem Benutzer, am Anfang einer Review die relevanten IT-Prozesse nach verschiedenen Kriterien zu selektieren, die dazugehörigen Kontrollen am Bildschirm anzuschauen und deren Wichtigkeit im zu analysierenden Fall zu bestimmen. Die Resultate der Analyse werden in Form einer synthetischen Bewertung (5-stufige Skala) neben jeder Kontrolle festgehalten. Wo nötig können zusätzlich Feststellungen, Empfehlungen und Management-Stellungnahmen erfasst werden. Verschiedene strukturierte Reports oder Graphiken stehen anschliessend zur Verfügung, um die Resultate darzustellen. Die Software kostet US\$ 600.-- (Adresse siehe oben).

Methodware Limited, PO Box 27415, Wellington, New Zealand

Tel.: +64 4 495 7302, Fax: +64 4 495 7400

E-mail: advisor@methodware.co.nz

Weitere Informationen auf der Internet-Homepage:

<http://www.methodware.co.nz>

- "COBIT Self Assessment" von Certification Training Institute (CTI) erlaubt dem Benutzer sein Stand bei der Implementation der COBIT-Kontrolle zu verifizieren und quantifizieren. Für jedes Kontrollziel sind fünf "Levels of Compliance" definiert und beschrieben. Die Resultate können auf verschiedene Art und Weise zusammengefasst werden. Die Software kostet US\$ 300.-- (Weitere Informationen im Internet). Eine erweiterte CD-ROM-Version des Produktes ist unter dem Name "COBIT Self Assessment Advisor" bei Methodware Ltd. (Kontaktangaben s. unter "COBIT Advisor") zum Preis von US\$ 1'400.-- erhältlich.

Certification Training Institute (CTI)

<http://www.cobit-sa.com/cobit.html>

9. Ausblick: Erweiterungen, Ergänzungen

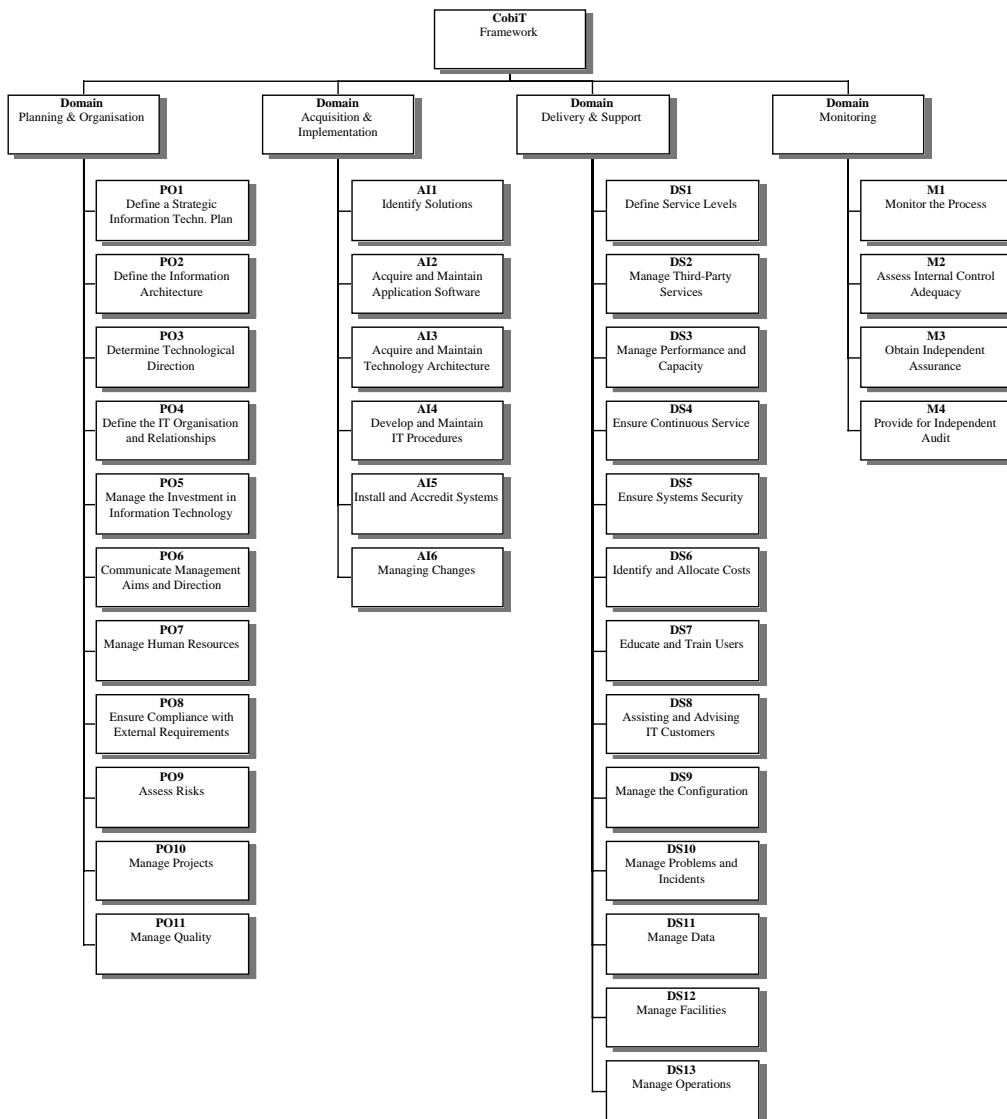
Die neueste Aktualisierung von COBIT brachte einige lang ersehnte Hilfsmittel, doch fehlen uns derzeit noch die breite Praxis-Erfahrungen damit. Die ersten Eindrücke sind jedoch durchaus positiv. Die riesige Informationsdatenbank auf der CD-ROM läuft derzeit nur unter Windows 3.x oder Windows 95, eine Mac-Version ist auf Herbst geplant (mit VirtualPC oder Softwindows funktioniert es bereits heute). Ebenfalls in der Pipeline ist noch ein "Process Performance Benchmark" für Self-Assessment.

10. Anwendungstips

Wenn man COBIT regelmässig einsetzen will und keine kommerzielle Software zur Verfügung hat, empfiehlt es sich die Kontrollziele in eine Datenbank zu erfassen. Selektionen, Bewertungen und Reports lassen sich so leicht und zeitsparend produzieren. Der Aufwand dafür hält sich in Grenzen, da alle Daten elektronisch verfügbar sind. Bei Kauf von COBIT ist dieses Vorgehen übrigens ausdrücklich erlaubt.

COBIT benötigt einen grösseren Initialaufwand. Es lohnt sich genügend Zeit aufzuwenden, bevor man COBIT vorschnell als unbrauchbar erklärt. Von COBIT soll auch nicht mehr verlangt als das was der Standard anbieten kann. COBIT soll für die Festlegung der Struktur und der übergeordneten Kontrollziele benutzt werden. Für die konkrete Bestimmung der Massnahmen sind eigene Anstrengungen nötig bzw. müssen andere Produkte beigezogen werden.

Die Struktur von COBIT



Marion



1. Geschichte

Marion (Méthode d'Analyse des Risques Informatiques et d'Optimisation par Niveau) wurde in Frankreich 1986 von den Herren J.-M. Lamère, Y. Le Roux und J. Tourly entwickelt und in ihrem Buch "La sécurité des réseaux; Methodes et techniques" 1989 beim Verlag Dunod publiziert. Marion ist eine Applikation zur Beurteilung der Informationssicherheit und basiert auf der gleichnamigen Methode, welche sich hauptsächlich in francophonen Gebieten etabliert und in vielen Unternehmen bis heute im praktischen Einsatz bewährt hat.

2. Vorstellung der Methode

Ein Vorteil dieser Methode ist, dass alle sicherheitsrelevanten Elemente konsequent quantifiziert werden. Verlässliches empirisches Datenmaterial unterstützt die Anwender bei Bewertungen und bei zutreffenden Entscheidungen. Für Auswertungs-, Optimierungs- und Simulationsrechnungen steht eine leistungsfähige Software zur Verfügung. Eine Untersuchung mit Marion läuft in drei Phasen ab:

- Phase 1, *Verletzbarkeitsstudie*, eruiert die möglichen Angriffe auf das Informatiksystem und ordnet sie in der Reihenfolge der Wahrscheinlichkeit ihres Auftretens in Anbetracht des vorhandenen Sicherheitsniveaus.
- Phase 2, *Analyse der Risiken*, erlaubt die Rangordnung der Auswirkungen und ihrer Tragweite.
- Phase 3, *Sicherheitsplan*, basiert auf den Ergebnissen der vorangegangenen Untersuchungen und ermöglicht es, der Geschäftsleitung folgendes zu unterbreiten:
 - Eine erste Liste relativ einfacher und kostengünstiger Massnahmen und Verfahren, deren Einsatz das Sicherheitsniveau verbessert und unmittelbar "gewinnbringend" ist (Verhältnis Kosten der Studie/erzielter Sicherheitsgewinn).
 - Eine Liste der tiefer greifenden vorrangigen Aktionen, die nach detaillierter Spezifikation eine sinnvolle Wahl der Verfahren, Produkte und Dienste erlauben, welche für die tatsächliche Begrenzung der in Phase 2 identifizierten wesentlichen Risiken erforderlich sind.

3. Hersteller/Lieferant

Die Lieferfirma ist Partenaire Sécurité Informatique. In der Schweiz gibt es zur Zeit keine Vertreter von PSI oder Verkäufer der MARION-Methode. Preise: Für die SW-Lizenz für die MARION-WINAP+ Methode ist mit einem einmaligen Betrag von ca. Sfr.11,000.-- zu rechnen. Die Software wird laufend aktualisiert. Für diesen

Partenaire Sécurité Informatique (PSI)

58, boulevard Gouvion Saint-Cyr

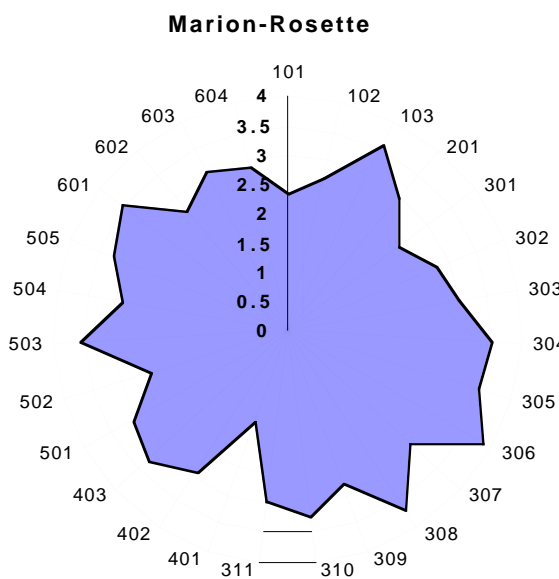
F 75858 Paris Cedex 17; Tel 0033 1 44 09 10 00

Support ist mit ca. Sfr. 1600.-- jährlich zu rechnen. Zusätzlich ist für die Schulung ein Aufwand von ca. drei Tagen einzuplanen, um die Methode selbständig anwenden zu können.

4. Hauptanwendungen Revision und Erstellung Sicherheitskonzept

Marion wird bevorzugt eingesetzt für die Durchführung von Risikoanalysen und die Erstellung von Sicherheitskonzepten. Zuerst werden mit strukturierten Interviews und vorgegebenen Risikoszenarien diejenigen Risiken identifiziert, welche die Fortführung der Geschäftstätigkeit beeinträchtigen könnten. Danach werden 27 Bereiche der Informationssicherheit anhand eines jährlich angepassten Fragebogens bewertet und graphisch dargestellt. Dies bedingt das Bewerten und Beantworten von ca. 800 relativ komplizierten Fragen. Zuletzt werden aus einer Erfahrungsdatenbank standardisierte Massnahmen vorgeschlagen. Diese werden in Form von funktionalen Anforderungen zusammen mit möglichen Implementationsvorschlägen dargestellt. Zusätzlich werden Sachkosten und personelle Aufwendungen als Schätzwerte berechnet.

5. Stärken und Schwächen



Seite der Rosette die allgemeinen Kontrollen (Management), die sozialökonomischen Faktoren sowie die generellen physischen Sicherheitsaspekte. Die linke Seite dagegen die logische Sicherheit, also die Sicherheit der Hard- und Software, der Produktion und der Systementwicklung. Die nach aussen gerichteten Strahlen über der Note 2 zeigen Sicherheitsfaktoren, die im Verhältnis der verschiedenen Vergleichsbranchen (Handel, Banken, Versicherungen, Industrie) relative gute Durchschnittswerte erzielen.

Die grosse Stärke dieser Methode liegt in der graphischen Darstellung der Ergebnisse zum Stand der Sicherheit des untersuchten Bereiches. Die Bewertung der 27 Sicherheitsfaktoren ist auf den Strahlen einer Rosette von innen nach aussen aufgetragen. Dabei bedeuten Note 0 (Zentrum) wenig oder keine Deckung; Note 4 (äusserster Kreis) sehr gute Deckung oder sogar einen Überschuss. Diese Graphik erlaubt, eine rasche Aussage über die Homogenität (beziehungsweise die Inhomogenität) der Sicherheitsvorkehrungen zu machen. Grob unterteilt repräsentiert die rechte

Die Faktoren der Marion-Rosette

- 101 Organisation structure and functions
- 102 Management controls
- 103 Security procedures and audit
- 201 Socio economics factors
- 301 Physical environment
- 302 Physical access control
- 303 Pollution
- 304 Safety instructions
- 305 Fire Protection
- 306 Water Protection
- ...

Die Methode kann nach entsprechender Ausbildung durch firmeneigene Mitarbeiter angewendet werden. Ein Vorteil liegt in der jährlichen Aktualisierung der elektronischen Fragebogen und der Möglichkeit der Anpassung an die firmeneigenen, sicherheitsrelevanten und spezifischen Zusatzrisiken.

Als Schwäche kann die Zertifizierbarkeit genannt werden. D.h. es ist methodisch nicht sichergestellt, dass man genau zum selben Resultat käme, wenn dieselbe Untersuchung mehrmals durchgeführt würde. Jeder neue Fragebogen wird zuerst auf französisch erstellt und später auf englisch übersetzt. Erfahrungsgemäss ist die englische Übersetzung recht mässig. Oft kann daher nicht auf Ebene der einzelnen Frage gearbeitet werden, sondern man muss sich auf Grund des übergeordneten Themas ein Bild des zu hinterfragenden Gegenstandes machen.

Wird die Methode wie vorgeschlagen eingesetzt, dauert das Sicherheitsprojekt ca. vier Monate und absorbiert je nach Betriebsgrösse erhebliche personelle Ressourcen, was als Nachteil beurteilt werden kann. Oft wird deshalb die vorgeschlagene Methodik drastisch verkürzt, indem man sich auf die Phase 2 konzentriert.

Die Faktoren der Marion-Rosette (Fortsetzung)

307 Reliability of the installation
 308 Disaster recovery procedures
 309 User liaison procedures
 310 EDP personal policies
 311 IT strategy
 401 Hardware and system security
 402 Telecomm security
 403 Data base security
 501 Storage and retrieval of data
 502 Data capture and transfer
 503 Backup
 504 Operations procedures
 505 HW and purchased SW maintenance
 601 Change control
 602 Analysis and programming methods
 603 Programmed controls
 604 SW package security

6. Denkbare andere Einsatzgebiete

Durch geschicktes Anpassen der 27 Sicherheitsfaktoren auf eigene Bedürfnisse und/oder durch die Ergänzung mit anderen Katalogisierungsmerkmalen (z.B. CoP, Grundschutzhandbuch, Checklisten usw.) dienen diese Vorgaben als Baseline zur Erstellung eines firmenspezifisches Sicherheitskonzeptes.

7. Nicht geeignet für ...

Weniger einzusetzen oder sogar ungeeignet ist die Marion-Methode für die Durchführung einer Informatik-Revision. Obwohl die von Marion generierten Massnahmen umfangreich sind, sind sie zu generell und zu oberflächlich, um ohne eine firmenspezifische Anpassung als Basis für ein Sicherheitshandbuch zu dienen.

8. Software-Unterstützung (Plattformen usw.)

Für die Durchführung einer Risikoanalyse wird die Software MARION-WINAP+ eingesetzt (Windows 3.1). Gemäss Aussagen der Hersteller ist eine Portierung auf weitere Plattformen nicht geplant. Die mit der Software Marion erarbeiteten Ergebnisse und Auswertungen werden elektronisch generiert.

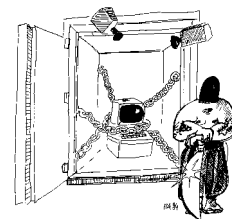
9. Ausblick: Erweiterungen, Ergänzungen

Die in ihren Ursprüngen wegweisende, leider nur auf den francophonen Markt ausgerichtete Methode verliert an Bedeutung. Durch den Weggang der führenden Initianten stagnieren die innovativen und zukunftsgerichteten Aspekte immer mehr. Obwohl Marion noch durch die CLUSIF (Club sécurité informatique Français) und durch die APSAD (Vereinigung französischer Versicherungsgesellschaften) getragen und als "de Facto-Standard" von diesen verbreitet wird, verliert sie in andern Ländern immer mehr an Bedeutung. Deshalb ist in nächster Zeit, ausser den regelmässigen Aktualisierungen, mit keinen nennenswerten methodischen Erweiterungen und Ergänzungen zu rechnen.

10. Anwendungstips

Für die Phase 2 hat sich bewährt, in einer Art round-table-Diskussion mit verschiedenen Vertretern des untersuchten Bereiches gleichzeitig den Fragebogen zu beantworten. Dabei sollte man Wert darauf legen, dass die Befragten unter sich zu einem Konsens kommen. Sehr hilfreich ist es zudem, wenn die Skalenwerte der Beurteilung (1-4) mit Stichworten oder kurzen Sätzen verdeutlicht werden. Vor dem Projektstart ist eine umfassende Instruktion der Betroffenen über die verschiedenen Projektphasen und die Marion-Methode unumgänglich.

IT-Grundschutzhandbuch

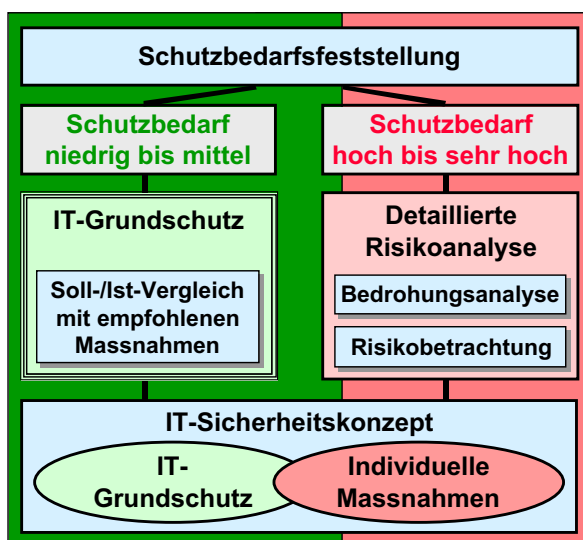


1. Geschichte

1992 publizierte das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) das Handbuch für die sichere Anwendung der Informationstechnik (IT-Sicherheitshandbuch). Darin wurde ein Verfahren beschrieben, mit dem der aktuelle Sicherheitsstatus eines IT-Einsatzes festgestellt und die IT-Sicherheit gewährleistet werden kann. Das Vorgehen wurde in die vier Stufen Ermittlung der Schutzbedürftigkeit, Bedrohungsanalyse, Risikoanalyse, Erstellung des IT-Sicherheitskonzeptes mit insgesamt 12 Schritten gegliedert.

In der Praxis setzte sich sehr rasch die Erkenntnis durch, dass dieses Verfahren in seiner Gesamtheit wohl richtig und unbestritten, in der Anwendung jedoch zu komplex und schwerfällig war. Insbesondere waren kleinere und mittlere Organisationen damit überfordert, sowohl bezüglich Know-how als auch Aufwand. So entstand 1995 das Nachfolgewerk "IT-Grundschutzhandbuch" (Massnahmenempfehlungen für den mittleren Schutzbedarf).

2. Vorstellung der Methode

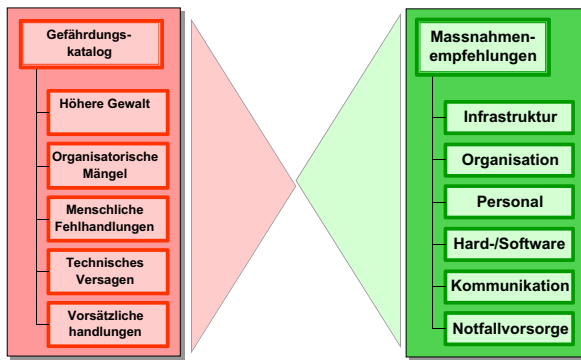


Zielsetzung dieser Methode ist, bei IT-Systemen ein Sicherheitsniveau zu erreichen, das für den mittleren Schutzbedarf angemessen und ausreichend ist und als Ausgangsbasis für hochschutzbedürftige IT-Anwendungen dienen kann.

Die Anwendung erfordert zwingend eine Schutzbedarfsfeststellung. Entsprechend der Zielsetzung ist die Methode nur für niedrigen bis mittleren Schutzbedarf direkt anwendbar. Das Verfahren wird ausführlich beschrieben und ist ohne Schwierigkeiten nachvollziehbar.

Die Methode ist als Baukasten konzipiert und enthält 27 Bausteine (siehe Kasten). Zu jedem dieser Bausteine werden eine standardisierte Gefährdungslage und die entsprechenden Massnahmen vorgegeben. Der Gefährungskatalog enthält die fünf Hauptgruppen:

- G1: Höhere Gewalt,
- G2: Organisatorische Mängel,
- G3: Menschliche Fehlhandlungen,
- G4: Technisches Versagen und
- G5: Vorsätzliche Handlungen.



Die Massnahmen ihrerseits werden in sechs Hauptkategorien zusammengefasst:

- M1: Infrastruktur,
- M2: Organisation,
- M3: Personal,
- M4: Hardware und Software,
- M5: Kommunikation und
- M6: Notfallvorsorge.

Die IT-Systeme, die entsprechend der Schutzbedarfsfeststellung für die Anwendung des IT-Grundschutzes geeignet sind, werden mit den dargestellten Bausteinen möglichst genau nachgebildet und mit dem Soll der empfohlenen Massnahmen verglichen.

Als Teilergebnisse entstehen damit Aktionspläne der zu realisierenden IT-Grundschutzmassnahmen pro Baustein. Das Gesamtergebnis ist die Konsolidierung dieser Aktionspläne in ein umfassendes IT-Grundschutz-Massnahmenkonzept.

3. Hersteller/Lieferant

Das "IT-Grundschutzhandbuch" wird publiziert vom Bundesamt für Sicherheit in der Informationstechnik, Referat VI 3, Postfach 200363, D-53133 Bonn.

Bezugsquelle

Jede gute Fachbuchhandlung oder direkt bei Bundesanzeiger Verlagsgesellschaft mbH, Postfach 100534, D-50445 Köln, Preis ca. DM 108.—

Dem Handbuch liegt seit der Ausgabe 1997 die elektronische Version im HTML- und Winword-Format bei. Zusätzlich werden die Erhebungsformulare und verschiedene Hilfsdokumente auf der CD-ROM mitgeliefert. Das Handbuch erscheint normalerweise Mitte Jahr in einer überarbeiteten und erweiterten Fassung.

4. Hauptanwendung

Die Hauptanwendung der Methode IT-Grundschutz liegt in der Unterstützung bei der Erarbeitung von IT-Sicherheitskonzepten/-teilkonzepten resp. den entsprechenden Handbüchern. Dies umfasst sowohl den organisatorischen Teil als auch die Ausformulierung konkreter Vorgaben und Massnahmen. Die Massnahmen können theoretisch 1:1 übernommen werden. Die Praxis zeigt, dass aus psychologischen, organisatorischen und politischen Überlegungen oftmals Anpassungen vorgenommen werden müssen. Wichtig ist, dass der IT-Sicherheitsprozess, auf dem die Methode basiert, initialisiert wird, bevor mit der Erarbeitung des IT-Grundschutzkonzeptes begonnen wird.

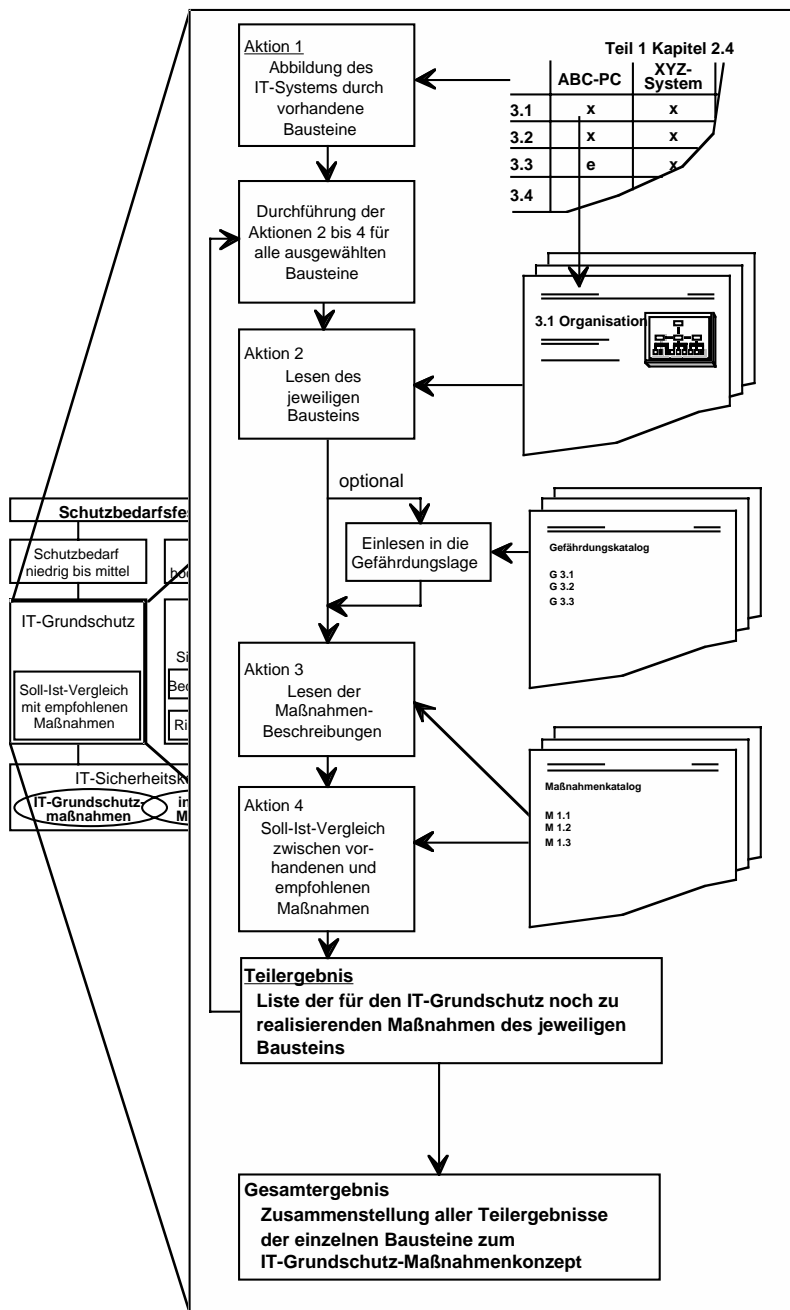
5. Stärken und Schwächen der Methode

Gegenüber dem ursprünglichen IT-Sicherheitshandbuch und vielen anderen Methoden entfällt die Bedrohungs- und Risikoanalyse. Dies erlaubt ein schnelles und effizientes Vorgehen. Langwierige und oft nutzlose Diskussionen über Gefährdungsszenarien

entfallen. Die vorgeschlagenen Massnahmen haben einen klaren Bezug zur Praxis. Im Vordergrund steht das schnelle Erreichen eines umfassenden mittleren Schutzniveaus.

Als Einstieg ist der Massnahmenkatalog Notfallvorsorge hervorragend geeignet. Das Thema ist einerseits in sich geschlossen, führt aber andererseits als Querschnittsfunktion sehr gut in die Thematik IT-Sicherheit und damit auch in die Methode IT-Grundschutz ein.

Es fehlt jedoch der konzeptionelle Überbau im Sinne einer Klammerfunktion für die einzelnen Bausteine. Der IT-Grundschutz ist nicht zielorientiert. Die Ziele kommen wohl implizit durch die ausgewählten Massnahmen zum Ausdruck. Mit einer Formulierung von insbesondere messbaren Zielvorgaben könnte die Motivation und auch die Nachvollziehbarkeit markant gesteigert werden.



6. Denkbare andere Einsatzgebiete

Die Methode IT-Grundschutz bietet dem Revisor einen praxisorientierten Input für die Erarbeitung entsprechender Revisionsprogramme. Die Methode selbst ist jedoch kein Audit-Programm im engeren Sinn.

Die Methode ist weiter auch durchaus geeignet, kleinere Selbstüberprüfungen vorzunehmen. Die entsprechenden Formulare sind vorhanden.

7. Nicht geeignet für ...

Die Methode IT-Grundschutz ist nicht geeignet für Risikoanalysen. Das Ziel der Methode ist letztlich die Vermeidung solcher Analysen.

8. Software-Unterstützung

Es sind verschiedene Tools im Entstehen. Eine Beurteilung ist im Moment nicht möglich. Das BSI wird in Zusammenarbeit mit der Firma Ploenzke ein entsprechendes Tool auf den Markt bringen.

9. Ausblick: Erweiterungen, Ergänzungen

Das BSI ist sehr daran interessiert, Beiträge aus der Praxis für die entsprechenden Erweiterungen des IT-Grundschutzhandbuchs zu erhalten. Dieser angestrebte Bezug zur Praxis ist eine grosse Stärke der Methode.

Das IT-Grundschutzhandbuch wird vom BSI im Internet zur Verfügung gestellt, wo auch weitere interessante Publikationen greifbar sind: www.bsi.bund.de/.

Das Baukastensystem (Stand Ausgabe 1997)

1 IT-Grundschutz übergeordneter Komponenten

- 1.1 Organisation
- 1.2 Personal
- 1.3 Notfallvorsorge-Konzept
- 1.4 Datensicherungskonzept
- 1.5 Datenschutz

2 IT-Grundschutz im Bereich Infrastruktur

- 2.1 Gebäude
- 2.2 Verkabelung
- 2.3 Räume
- 2.4 Schutzschranke

3 Nicht vernetzte Systeme

- 3.1 DOS-PC (Ein-Benutzer)
- 3.2 Unix-System
- 3.3 Tragbarer PC
- 3.4 DOS-PC (mehrere Benutzer)
- 3.5 PC unter Windows NT
- 3.6 PC mit Windows 95

4 Vernetzte Systeme

- 4.1 Servergestütztes Netz
- 4.2 Vernetzte Unix-Systeme
- 4.3 Peer-to-Peer-Netz
- 4.4 Windows NT Netz
- 4.5 Novell Netware 3.x

5 Datenübertragungseinrichtungen

- 5.1 Datenträgeraustausch
- 5.2 Modem
- 5.3 Firewall

6 Telekommunikation

- 6.1 TK-Anlage
- 6.2 Fax-Gerät
- 6.3 Anrufbeantworter

7 Sonstige IT-Komponenten

- 7.1 Standardsoftware

10. Anwendungstips

Die auf der CD-ROM vorhandenen Erhebungsformulare können mit relativ kleinem Aufwand übernommen werden. Die Schutzbedarfsfeststellung führt bei der praktischen Durchführung sehr rasch zu positiven Sensibilisierungseffekten.

Die Resultate der Umfrage



Ausgangslage

Jede Organisation ist vor die Aufgabe gestellt, mögliche Verlustrisiken zu erkennen, Massnahmen zu ihrer Begrenzung einzuleiten, deren Durchführung zu überwachen und Anpassungen an die sich verändernden Umweltsituationen zu veranlassen. Durch Einsatz von Hilfsmitteln beispielsweise für die Durchführung von Risikoanalysen oder die Erstellung von Sicherheitskonzepten kann diese Aufgabe wesentlich erleichtert werden.

Die Interessengruppe CoP hat sich dazu entschlossen, einige der auf dem Markt verfügbaren Hilfsmittel etwas näher anzuschauen. Im Herbst 1997 wurden neben den 600 Mitgliedern von SWISS-ISA (ISACA Switzerland Chapter, Clusis, SI Security) weitere 100 Einzelpersonen angeschrieben und gebeten, an der Umfrage über die von ihnen eingesetzten Methoden für die Durchführung von Revisionen, Healthcheck und Risikoanalysen sowie für die Erstellung von Sicherheitskonzepten und Sicherheitshandbüchern teilzunehmen.

Mit insgesamt rund 170 Einzelmeldungen sind die in diesem Beitrag aufgeführten Aussagen statistisch nicht immer über alle Zweifel erhaben, doch lassen sich in den meisten Fällen Trends erkennen. Die von uns gezogenen Schlussfolgerungen sind mit der notwendigen Vorsicht zu geniessen. Da alle Mitglieder der IG CoP über (teils jahrelange) Erfahrung mit zwei oder mehr der untersuchten Methoden verfügen, konnten wir die "statistischen" Erkenntnisse mit unseren eigenen Erfahrungen überprüfen und grösstenteils bestätigen.

Mit der Umfrage wollte die Interessengruppe folgende Ziele erreichen:

- Vergleich der in der Praxis angewendeten Methoden
- Bestimmung des geeigneten Anwendungsbereiches
- Abklärung der Einsatzhäufigkeit
- Bestimmung der Anforderungen an Methoden
- Erarbeiten der Entscheidungshilfen für Methodenauswahl

Die Umfrage erfolgte mit zwei Fragebogen. Mit dem ersten (Teilumfrage A) sollten die mit CoP, COBIT, Marion und dem Grundschutzhandbuch gemachten Erfahrungen gesammelt werden. Mit dem zweiten (Teilumfrage B) wurden unabhängig von den vier vorgestellten Methoden die Wünsche für eine "optimale" Methode gesammelt.

Erläuterungen zu den "Anwendungsbereichen"

Risikoanalyse

Methodische Ermittlung aller Risiken eines Systems durch Abschätzung der Eintretenswahrscheinlichkeit eines schädigenden Ereignisses und des damit verbundenen Schadenausmasses.

Revision

Unabhängiger, neutraler Vergleich zwischen dem tatsächlichen und dem vorgegebenen Zustand (Soll/Ist-Vergleich) eines Regelwerks hinsichtlich seiner Zweck-eignung und/oder Einhaltung.

Sicherheitskonzept

Systematische Festlegung der konzeptionellen Sicherheitsanforderungen und dem Vorgehen zu ihrer Umsetzung in Massnahmen.

Sicherheitshandbuch

Nachvollziehbare Festlegung bzw. Umsetzung der im Sicherheitskonzept festgehaltenen Anforderungen in konkrete Massnahmen.

Healthcheck

Rasch durchführbare Standortbestimmung bezüglich der Informationssicherheit.

Die Ergebnisse der Teilmfrage A auf einen Blick

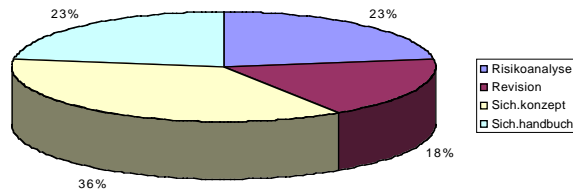
Die Teilnehmer wurden gebeten anzugeben, welche der Methoden CoP, COBIT, Marion und Grundschutzhandbuch sie für welche der Anwendungen Risikoanalyse, Revision, Sicherheitskonzept und Sicherheitshandbücher einsetzen. Anzugeben war im weiteren, ob dafür Software eingesetzt wurde, ob dies für die eigenen Unternehmung oder für Dritte geschah und wie umfangreich ihre Erfahrung damit ist.

Die Resultate der 101 Einzelbewertungen sind auf den ersten Blick nicht überraschend: So eignet sich z.B. Marion gut für Risikoanalysen und das Grundschutzhandbuch für die Erstellung von Sicherheitshandbüchern. Im weiteren wurden bestehende Vorurteile zementiert: So ist COBIT etwas für die Revision, CoP geeignet für alles und Marion immer ein riesiger Aufwand.

	Code of Practice	COBIT	Marion	Grundschutzhandbuch
bevorzuge Anwendungen	primär Erstellung von Sicherheitskonzepten; aber in allen Anwendungen häufig	Revisionen	Risikoanalysen Erstellung von Sicherheitskonzepten	Erstellung von Sicherheitskonzepten und Sicherheitshandbüchern
weniger eingesetzt für		Erstellung von Sicherheitskonzepten und Sicherheitshandbüchern	Revisionen Erstellung von Sicherheitshandbüchern	Risikoanalysen Revisionen
Stärken	Unabhängigkeit Standardisierung Zertifizierbarkeit	Unabhängigkeit Standardisierung	Resultatdarstellung	Unabhängigkeit Anpassbarkeit Aktualisierung
Schwächen	Resultatdarstellung	Resultatdarstellung Anwenderfreundlichkeit	Zertifizierbarkeit	Resultatdarstellung
Bewertung (1 = schlecht, ..., 4 = ideal)	eher hoch (3.0)	eher hoch (3.0)	mittel (2.5)	eher hoch (3.0)
Bemerkungen	CoP ist auf Informationssicherheit fokussiert und wird daher gerne als Basis für Sicherheitskonzepte verwendet (vor allem in Europa).	COBIT deckt neben der Sicherheit auch Qualität und Zuverlässigkeit ab; ist aber wahrscheinlich ausserhalb der Revision noch wenig bekannt.	Marion ist ausserhalb Frankreich eher wenig verbreitet; wird aber z.B. von schweizerischen Unternehmen für "schnelle" Risikoanalysen verwendet.	Wird in erster Linie als Nachschlagewerk für die Wahl und Implementation von Sicherheitsmassnahmen verwendet. Eine eingebaute Risikoanalyse fehlt.

Leider konnten wir aus zeitlichen Gründen nicht mit allen Einsendern Gespräche führen; die Diskussionen innerhalb und ausserhalb der Interessengruppe zeigten jedoch klar auf, dass viele dieser Vorurteile auf fehlenden Informationen beruhen. Konsultiert man Personen mit einem breiten Erfahrungshintergrund im Einsatz dieser Methoden, so tritt Überraschendes zu Tage: Marion wurde beispielsweise von mehreren schweizerischen, aber international tätigen Unternehmen für rasche Risikoanalysen resp. Healthcheck eingesetzt, die nur wenige Tage dauerten und vorwiegend der Sensibilisierung dienen. Und der sogenannte "Revisionsstandard" COBIT ist bereits innert etwa eineinhalb Jahren nach seinem Erscheinen die Basis für die internen Sicherheitsrichtlinien von mehreren, ebenfalls international ausgerichteten Unternehmen in der Schweiz.

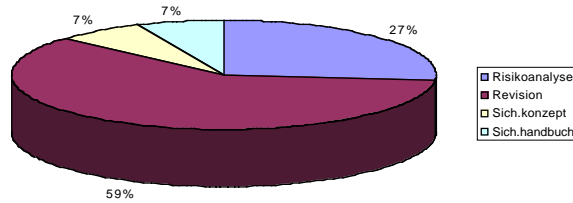
Code of Practice



Nicht überraschend ist die Verwendung des CoP zur Erstellung von Sicherheitskonzepten. Leicht weniger häufig wurde der CoP für Risikoanalysen und die Erstellung von Sicherheitshandbüchern verwendet. Auf dem vierten Platz aber immer noch erstaunlich hoch ist die Anwendung für Revisionen (18%).

Bei COBIT fällt die Fokussierung auf die Revision ins Auge – dies entspricht den Erwartungen. Erstaunliche 27% setzten aber bereits die erste Version von COBIT für Risikoanalysen ein, obwohl diese Anwendung erst mit der überarbeiteten Version von den Herausgebern propagiert wurde.

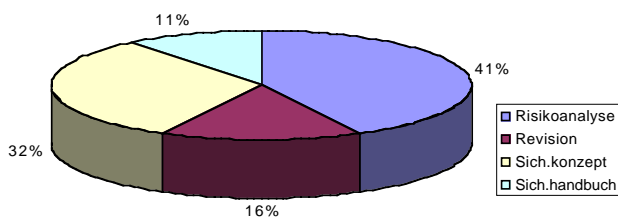
CobIT



Da COBIT ein umfassender Standard für Sicherheit und Qualität in der gesamten Informationstechnologie ist, erstaunt die (noch) kleine Zahl von Anwendungen für die Erstellung von Sicherheitskonzepten und Sicherheitshandbüchern.

Der Einsatz von Marion für Risikoanalysen entspricht dem "offiziellen" Ansatz. Marion ermöglicht auch den Ausdruck des umfassenden Fragebogens in einer Form, der als Basis für ein Sicherheitskonzept dienen könnte, womit sich die immerhin 32% erklären lassen.

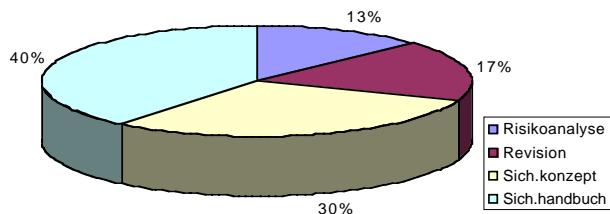
Marion



Als sauber strukturierter Leitfaden eignet sich Marion (wie die meisten derartiger Standards) auch als Basis von Revisionen. Wer Marion wirklich kennt, ist etwas erstaunt von der angegebenen Eignung für die Erstellung von Sicherheitshandbüchern (11%).

Beim IT-Grundschutzhandbuch des BSI ist die Eignung für die Erstellung von Sicherheitshandbüchern (40%) oder Sicherheitskonzepten (30%) offensichtlich.

Grundschutz-HB



Interessant wäre es für die meisten Mitglieder der Interessengruppe CoP, herauszufinden, warum sich das Grundschutzhandbuch für die Durchführung von Risikoanalysen oder von Revisionen eignen soll.

Die obigen Ergebnisse mögen noch so interessant sein; sie wurden durch die aktuellen Entwicklungen doch etwas überholt. COBIT 2nd edition unterstützt den Anwender zum Beispiel mit Hilfe zahlreicher Formulare und Denkansätze auch bei der Durchführung von Risikoanalysen und der Code of Practice wird zur Zeit massiv überarbeitet. Die Resultate der Umfrage können aber helfen bei der Wahl einer geeigneten Methode für die verschiedenen Anwendungsarten.

Im zweiten Abschnitt mussten die Teilnehmer der Umfrage angeben, wie gut die von ihnen eingesetzte Methode abschnitt bezüglich der zehn "Vergleichskriterien" Standardisierung, Unabhängigkeit, Zertifizierbarkeit, Umsetzbarkeit, Anpassbarkeit, Beurteilungsumfang, Resultatdarstellung, Wirtschaftlichkeit, Aktualisierung und Anwenderfreundlichkeit (siehe Kasten).

Die zehn Kriterien sind nicht objektiv messbar; es ist wenig erstaunlich, dass sie teilweise höchst unterschiedlich beurteilt wurden. Wir haben daher in der nachfolgenden Übersicht für alle Methoden diejenigen Kriterien aufgeführt, bei denen die Bewertungen übereinstimmend ausfielen (Standardabweichung < 0.80). Interessant ist daran, dass sich die Teilnehmer bei Marion nur über drei oder beim CoP über vier der zehn Kriterien einig waren, während es bei COBIT neun von zehn waren!

Code of Practice

- Standardisierung
- Unabhängigkeit
- Zertifizierbarkeit
- Umsetzbarkeit

COBIT

- Standardisierung
- Unabhängigkeit
- Umsetzbarkeit
- Anpassbarkeit
- Beurteilungsumfang
- Resultatdarstellung
- Wirtschaftlichkeit
- Aktualisierung
- Anwendungsfreundlichkeit

Marion

- Standardisierung
- Zertifizierbarkeit
- Resultatdarstellung

Grundschutzhandbuch

- Unabhängigkeit
- Umsetzbarkeit
- Anpassbarkeit
- Resultatdarstellung
- Wirtschaftlichkeit
- Aktualisierung

Erläuterungen zu den "Vergleichskriterien"

Standardisierung

Verwendung von international abgestützten Methoden und Verfahren. Breite internationale fach- und führungsbezogene Anerkennung. Methoden, Verfahren und Resultate sind in Anwendung und Darstellung standardisiert.

Unabhängigkeit

Die Methode kann grundsätzlich unabhängig, das heisst ohne Beizug von vorgegebenen Dritten (z.B. Hersteller, Berater) angewandt werden.

Zertifizierbarkeit

Die Methode lässt eine Zertifizierung von ihren Anwendern durch Dritte anhand von objektiven Verfahren grundsätzlich zu.

Umsetzbarkeit

Methode und Resultate sind praxis- und massnahmenbezogen. Sie lassen sich unmittelbar in konkrete Massnahmen umsetzen.

Anpassbarkeit

Methode und Resultate sind für alle Unternehmensgrößen und Strukturen anwendbar. Sie sind mit angemessenem Aufwand inhaltlich auf spezifische Unternehmensbedürfnisse anpassbar (z.B. durch modularen Aufbau von Methode und Resultatdarstellung).

Beurteilungsumfang

Die Methode stellt die Bearbeitung einer vollständigen Themenbreite zur Verfügung. Die Methoden und Verfahren sind in ihrer Bearbeitungstiefe und -breite vgängig skalierbar.

Resultatdarstellung

Die Methode unterstützt eine übersichtliche und rasch verständliche Darstellung der erzielten Resultate.

Wirtschaftlichkeit

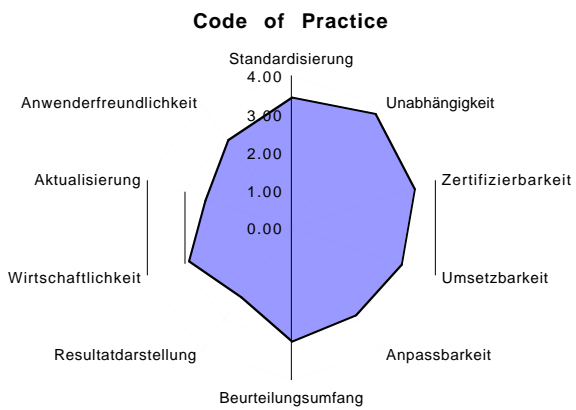
Die Methode führt innerhalb angemessener Zeit zu Resultaten. Das Aufwand-Nutzen Verhältnis ist transparent und nachvollziehbar (Management, Revision).

Aktualisierung

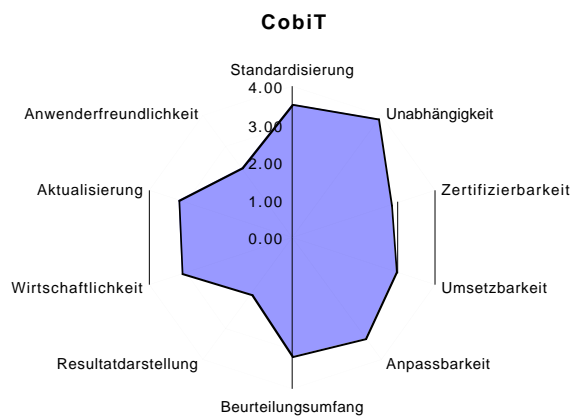
Der Inhalt wird regelmässig aktualisiert bzw. erweitert. Jeder neue Release ist mit seinem direkten Vorgänger kompatibel.

Anwenderfreundlichkeit

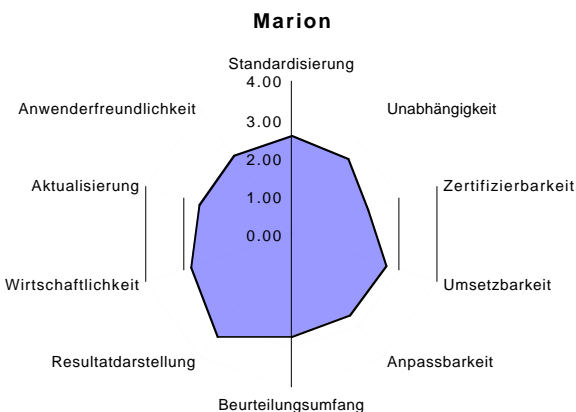
Die Methode lässt sich ohne grossen Lernaufwand nutzen, unterstützt die Arbeitsweise des Anwenders und verhält sich robust.



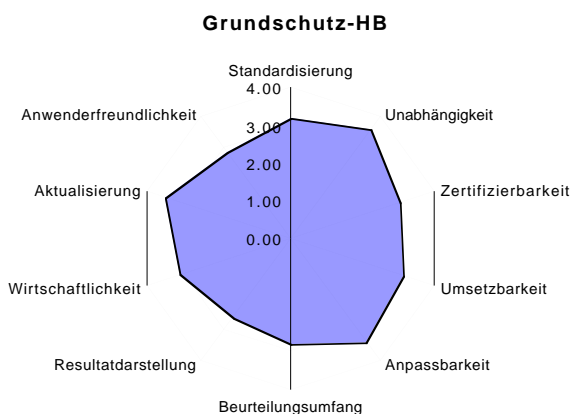
Beim Code of Practice fällt auf, dass die Unabhängigkeit des Herstellers (British Standards Institute) sehr geschätzt wird. Und obwohl in der Schweiz eine Zertifizierung wie in England nicht möglich ist, wird diesem Aspekt doch besondere Beachtung verliehen. Am unbefriedigendsten ist die Resultatdarstellung (Diese Aussage gilt etwas vermindert für diejenigen Personen, welche die Software CoP-iT einsetzen).



Bei COBIT sticht die Unabhängigkeit des Herstellers/Herausgebers noch deutlicher heraus als beim CoP; die Standardisierung wird ähnlich gewichtet. COBIT gilt als wenig anwenderfreundlich und die Resultatdarstellung schneidet noch schlechter ab. Dies dürfte sich wohl mit der 2nd edition etwas verbessern.



Bei Marion sind die Ergebnisse sehr ausgewogen aber bis auf die Resultatdarstellung in keinem Bereich herausragend. Es erstaunt etwas, dass eine Methode mit rundum nicht überzeugenden Bewertungen vor allem in Frankreich eine so grosse Beachtung fand und immer noch findet.



Das Grundschutzhandbuch besticht durch die laufende Aktualisierung, durch die Unabhängigkeit des Herausgebers (Bundesamt für Sicherheit in der Informationstechnik, Deutschland) und die leichte Anpassbarkeit an eigene Bedürfnisse. Nicht überzeugend ist die Anwenderfreundlichkeit und die Darstellung der Resultate.

Die Ergebnisse der Teilmfrage B auf einen Blick

Zum zweiten Teil der Umfrage (Wünsche an eine neue Methode) sind leider nur 73 Einzelbewertungen eingegangen, so dass die Ausführung hier nur teilweise aussagekräftig sind. Es lassen sich aber Trends identifizieren, die wir kurz zusammenfassen:

- Alle Anforderungsprofile sind sehr ähnlich. Abweichungen sind nicht unbedingt statistisch zu erhärten.
- Gesucht wird in erster Linie eine Methode für Revision. Ob diese Antwort so ausgefallen ist, weil vor allem die Revisionspezialisten den Fragebogen B ausgefüllt haben, ist nicht bekannt.
- Gewünscht wird auch eine Methode für Healthcheck (beim Fragebogen A wurde diese Variante nicht aufgeführt).
- An die Umsetzbarkeit und Anwenderfreundlichkeit werden generell hohe Anforderungen gestellt.
- Der Zertifizierung wird generell eher wenig Bedeutung beigemessen. Dies gilt auch für die Unabhängigkeit des Herausgebers/Herstellers.
- Die Anpassbarkeit an die eigenen Bedürfnisse scheint wichtig zu sein.

Risikoanalyse

- Wer eine Risikoanalyse durchführen möchte, stellt generell hohe Anforderungen an fast alle Kriterien. Die Unabhängigkeit der Hersteller und die Wirtschaftlichkeit spielt eine etwas kleinere Rolle; die Zertifizierung ist deutlich weniger wichtig.

Healthcheck

- Das Profil für Healthcheck ist zu demjenigen der Risikoanalyse fast identisch. Einzig die Zertifizierung ist von grösserer Bedeutung.

Revision

- Das Anforderungsprofil der Revision ist zu demjenigen der Risikoanalyse sehr ähnlich, doch spielt die Unabhängigkeit des Herstellers eine grössere und die Wirtschaftlichkeit eine etwas kleinere Rolle.

Sicherheitskonzept

- Bei der Erstellung von Sicherheitskonzepten scheint die Wirtschaftlichkeit leicht weniger wichtig zu sein. Deutlich weniger hohe Anforderungen bestehen bezüglich der Zertifizierbarkeit.

Sicherheitshandbuch

- Das Anforderungsprofil für eine Methode zur Erstellung des Sicherheitshandbuchs unterscheidet sich von einer für Sicherheitskonzepte praktisch nur die reduzierte Bedeutung der Unabhängigkeit.

