Zürcher Hochschule
für Angewandte Wissenschaften
zh aw School of Engineering
INE Institut für
Nachhaltige Entwicklung

IT-Risikoanalyse

Ralf Mock, 5. Oktober 2015

Lernziele

Die Teilnehmenden können

- wesentliche Merkmale von IT-Audits und -Risikoanalysen angeben und zusammenfassen
- für ihren beruflichen Alltag eine passende Methode auswählen und die Wahl begründen

Allgemeines

Die folgenden Standards und Methoden

- strukturieren die Aufgabe, komplexe IT-Systeme zu analysieren
- liefern allgemeingültige Checklisten / Kataloge zu Gefährdungen, Schwachstellen
- definieren allgemeingültige Massnahmen (verschiedene Unternehmensebenen)
- sind (auch) Werkzeuge des IT-Managements in Unternehmen

Anmerkung

Die Liste der vorgestellten Methoden ist nur eine Auswahl.

Methodisch

- Ansätze gelten als praxisnah, d.h. sie sind „quick & dirty“ und damit heuristisch & verzerrt
  - **heuristisch** ((heuristic): Methode, um komplexe Probleme, die sich nicht vollständig lösen lassen, mit Hilfe einfacher Regeln und unter Zuhilfenahme nur weniger Informationen zu entwirren. (aus: Wikipedia)
  - **verzerrt** (biased): Tendenz oder Vorliebe in Richtung auf bestimmte Sichtweisen, Anschauungen oder Ergebnisse (bewusste oder unbewusste subjektive Einschätzungen einer Person gehen als systematischer Fehler in die Analyse ein)
- Ergebnisse sind schlecht reproduzierbar (subjektiv, da vom Analytiker abhängig)
- generell mit hohem (Initial-)Aufwand verbunden

Code of Practice for Information Security Management

- Der „Information technology — Code of practice for information security management„ [1] legt allgemein Sicherheitsanforderungen der IT-Security in einem Unternehmen fest (im Sinne von Grundschutz; Baseline Approach).
- Die vorherige Version ISO/IEC 17799:2005 wurde 2007 umnummeriert in ISO/IEC 27002:2005, um den Standard in die ISO/IEC 27000-Standards einzugliedern. Der Inhalt blieb identisch.
- Ab ISO/IEC 17799:2005 hat der Code of Practice einen stärkeren Bezug zum Risiko-Management als frühere Versionen und baut auf den Definitionen des ISO/IEC GUIDE 73:2002 „Risk Management – Vocabulary – Guidelines for Use in Standards“ [2] auf. Damit ist die IT Security in den Definitionsrahmen der etablierten Risikoanalytik eingebettet.
- ISO/IEC 27001:2005 „Information technology – Security techniques – Specification for an Information Security Management System„ ist der Standard zur Zertifizierung von Information Security Management Systems von Unternehmen.

Gliederung ISO/IEC 27002

0. Introduction
1. Scope
2. Terms and Definitions
3. Structure of this Standard
4. Risk Assessment and Treatment
5. Security Policy
6. Organizing Information Security
7. Asset Management
8. Human Resources Security
9. Physical and Environmental Security
10. Communications and Operations Management
11. Access Control
12. Information Systems Acquisition, Development and Maintenance
13. Information Security Incident Management
14. Business Continuity Management
15. Compliance.

Objective – Control – Implementation Guidance

10.2 Third party service delivery management

Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

The organization should check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed with the third party.

10.2.1 Service delivery

Control

It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

Implementation guidance

Service delivery by a third party should include the agreed security arrangements, service definitions, and aspects of service management. In case of outsourcing arrangements, the organization should plan the necessary transitions (of information, information processing facilities, and anything else that needs to be moved), and should ensure that security is maintained throughout the transition period.

The organization should ensure that the third party maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster (see 14.1).

Anwendungszweck

- Erstellen eines konsistenten Sicherheitskonzeptes in Unternehmen bei grosser Nähe an die betriebliche Praxis
- Eignet sich weniger zur Erstellung eines Sicherheit-shandbuches, da der Detailierungsgrad zu grob ist und konkrete Umsetzungsmassnahmen meist fehlen.

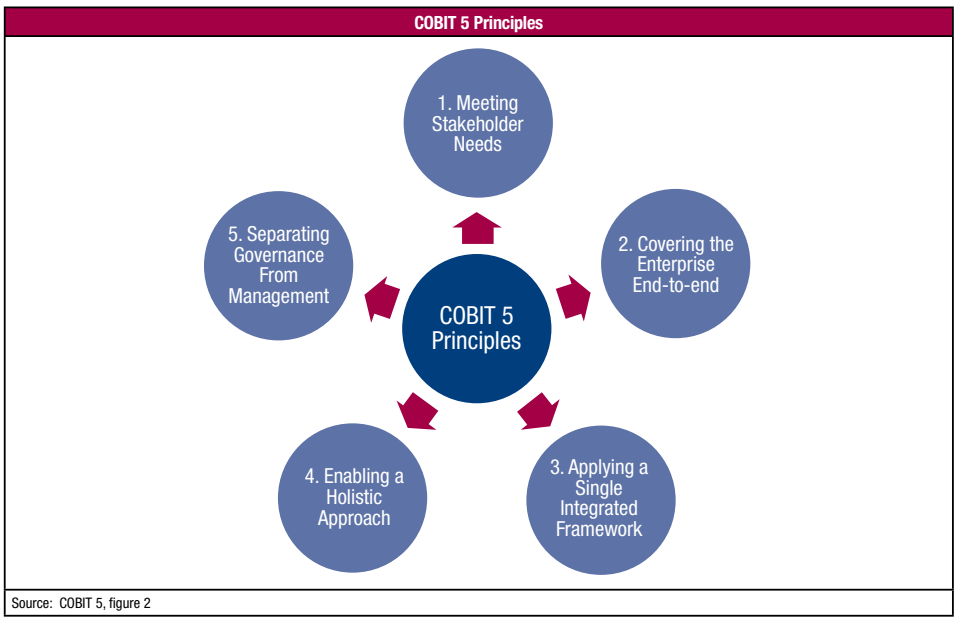
weitere Einsatzgebiete

Hilft beim Aufbau relativ einfacher Checklisten (z.B. FMEA-ähnlich) zur Abschätzung allgemeiner Risiken. Die Analayse zeigt dann die Differenz zwischen den implementierten IT-Security-Massnahmen zum Idealbild des Standards.

COBIT 5: Control Objectives for IT

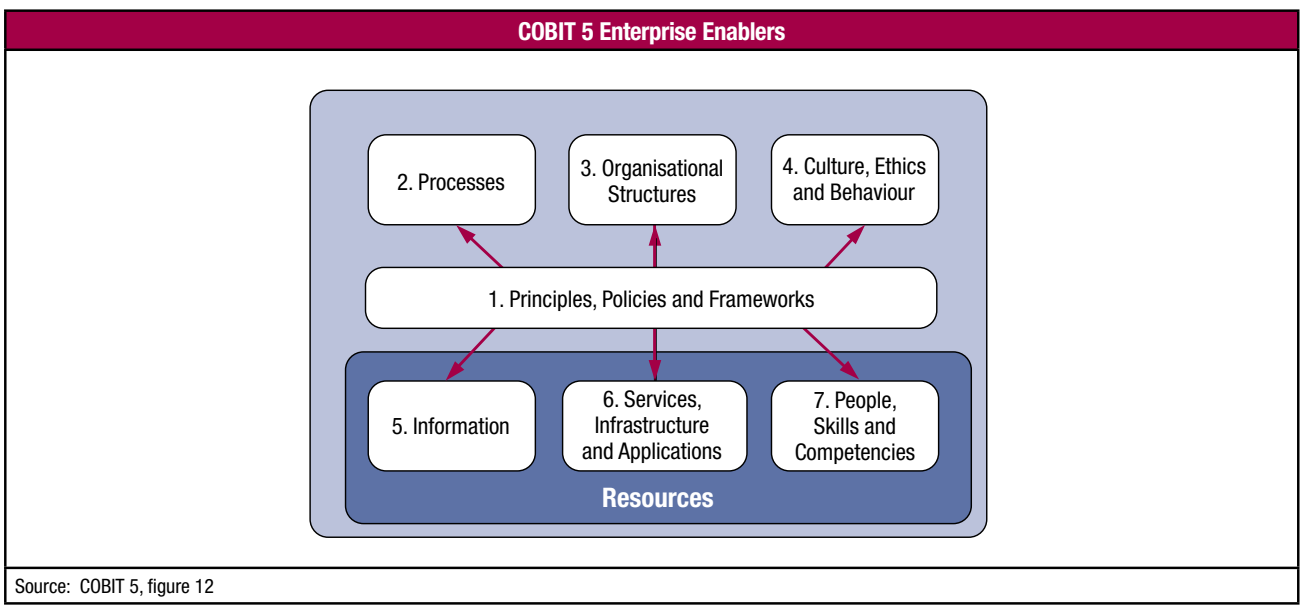
„COBIT 5 helps enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. The framework addresses both business and IT functional areas across an enterprise and considers the IT-related interests of internal and external stakeholders.(Herausgeber: Information Systems Audit and Control Association: [www.isaca.org/COBIT/Pages/default.aspx]

Prinzipien



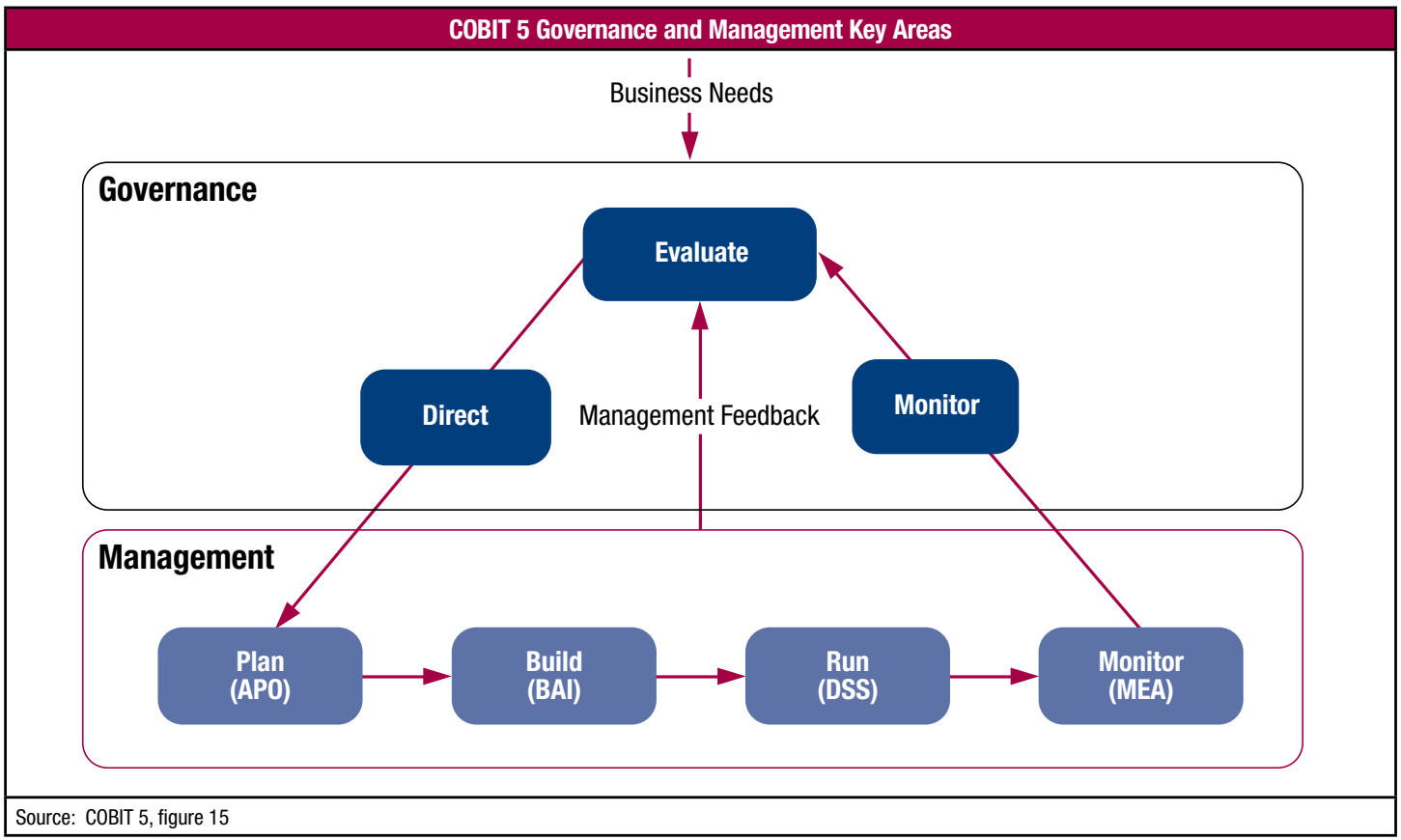
Prinzipien

1. **Meeting Stakeholder needs:** Unternehmen existieren, wenn sie einen Mehrwert generieren können.
2. **Covering the Enterprise end-to-end:** Betrachtung der Governance und des Managements von Informationen aus einer unternehmensweiten Sicht.
3. **Applying a Single Integrated Framework:** COBIT 5 positioniert sich als Integrationsframework für andere Standardwerke.
4. **Enabling a Holistic Approach:** Governance wird durch sog. *Enablers* beeinflusst.



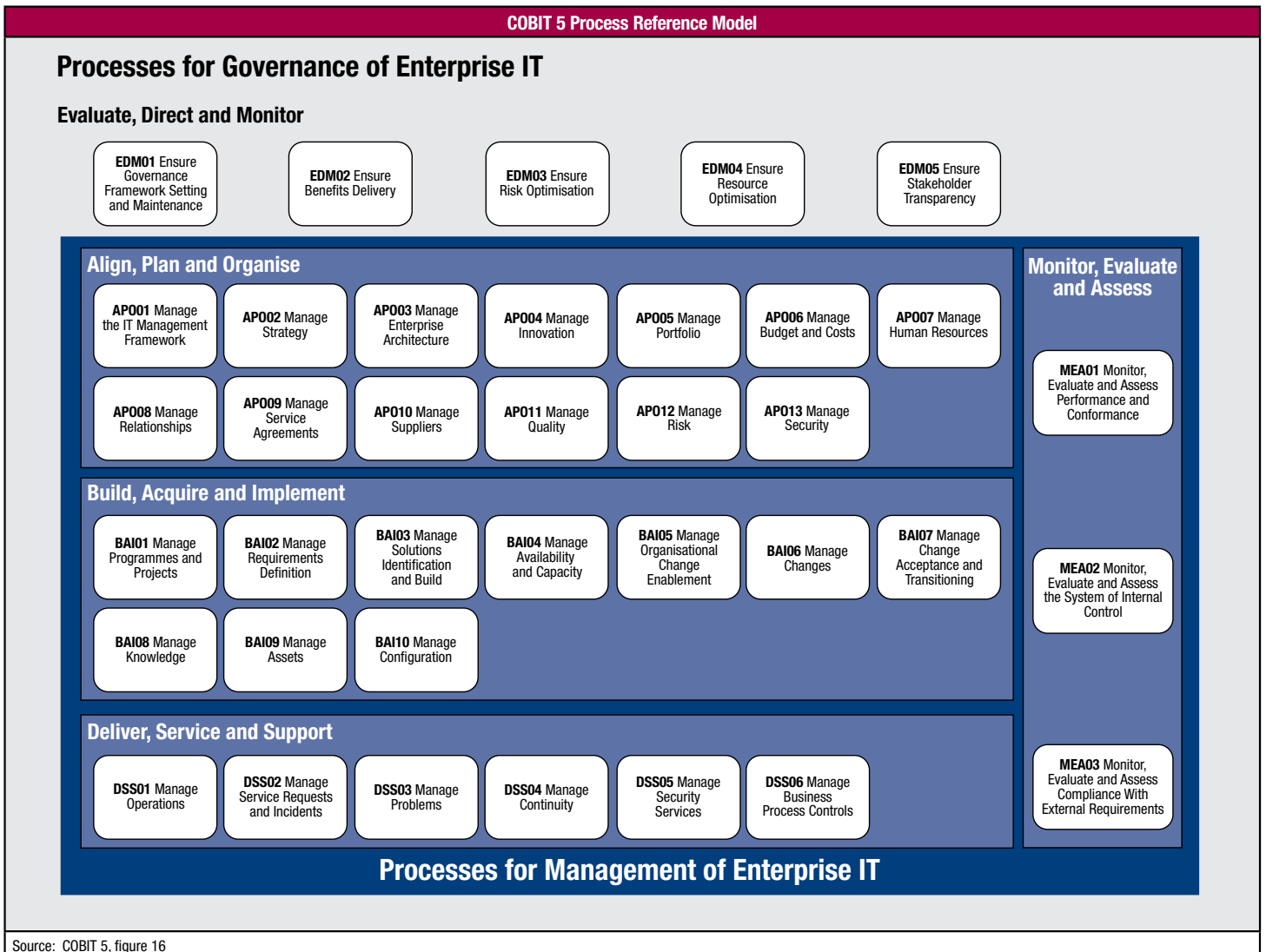
Prinzipien

5. **Separating Governance from Management:** Klare Unterscheidung zwischen Governance und Management. Unterteilt in *key areas*.



Source: COBIT 5, figure 15

Governance-Prozesse: Unterteilung der *key areas*



Source: COBIT 5, figure 16

Beispiel: Unterteilung des Prozesses DSS02

DSS02 Manage Service Requests and Incidents	Area: Management Domain: Deliver, Service and Support
Process Description Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; an record, investigate, diagnose, escalate and resolve incidents.	
Process Purpose Statement Achieve increased productivity and minimise disruptions through quick resolution of user queries and incidents.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. IT-related services are available for use.	• Number and percent of incidents causing disruption to business-critical processes • Mean time between incidents according to IT-enabled service
2. Incidents are resolved according to agreed-on service levels.	• Percent of incidents resolved within an agreed-on/acceptable period of time
3. Service requests are dealt with according to agreed-on service levels and to the satisfaction of users.	• Level of user satisfaction with service request fulfilment • Mean elapsed time for handling each type of service request

Quelle zu DSS02-Beispiel: [blog.itil.org/category/cobit/]

Beispiel: Unterteilung des Prozesses DSS02 nach Verantwortlichkeiten

DSS02 RACI Chart

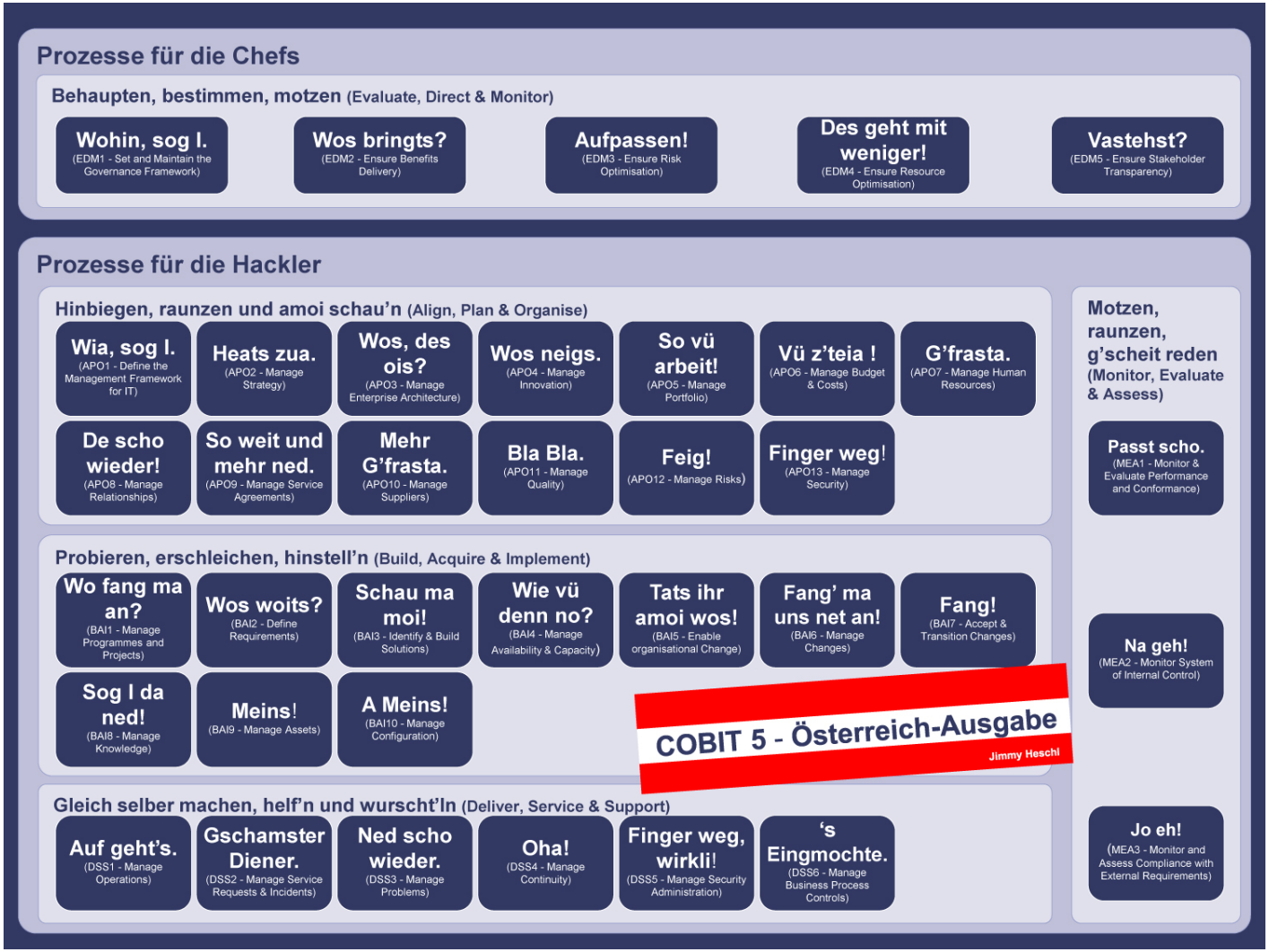
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS02.01 Define incident and service request classification schemes.						C					I	I						A	C	R	R		R	C	C	C
DSS02.02 Record, classify and prioritise requests and incidents.						I					I	I									A		R			I
DSS02.03 Verify, approve and fulfil service requests.						R												I		R	R		A			
DSS02.04 Investigate, diagnose and allocate incidents.						R					I	I				I	I	I		C	R		A	C		
DSS02.05 Resolve and recover from incidents.						I					I	I				C	C	I		R	R		A	R		C
DSS02.06 Close service requests and incidents.						I					I	I				I	I	I		I	A		I	R		I
DSS02.07 Track status and produce reports.						I					I	I				I	I	I		I	A		R	I		

R: Responsible; A: Accountable; C: Consulted; I: Informed

Beispiel: Incident Management Prozesse für DSS02

DSS02 Process Practices, Inputs/Outputs and Activities *(cont.)*					
Management Practice	**Inputs**		**Outputs**		
	From	**Description**	**Description**	**To**
DSS02.02 Record, classify and prioritise requests and incidents. Identify, record and classify service requests and incidents, and assign a priority according to business criticality and service agreements.	APO09.03	SLAs	Incident and service request log	Internal
	BAI04.05	Emergency escalation procedure	Classified and prioritised incidents and service requests	APO08.03 APO09.04 APO13.03
	DSS01.03	• Incident tickets • Asset monitoring rules and event conditions		
	DSS05.07	Security incident tickets		
Activities				
1. Log all service requests and incidents, recording all relevant information so that they can be handled effectively and a full historical record can be maintained.				
2. To enable trend analysis, classify service requests and incidents by identifying type and category.				
3. Prioritise service requests and incidents based on SLA service definition of business impact and urgency.				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
DSS02.03 Verify, approve and fulfil service requests. Select the appropriate request procedures and verify that the service requests fulfil defined request criteria. Obtain approval, if required, and fulfil the requests.	APO12.06	Risk-related root causes	Approved service requests	BAI06.01
			Fulfilled service requests	Internal
Activities				
1. Verify entitlement for service requests using, where possible, a predefined process flow and standard changes.				
2. Obtain financial and functional approval or sign-off, if required, or predefined approvals for agreed-on standard changes.				
3. Fulfil the requests by performing the selected request procedure, using, where possible, self-help automated menus and predefined request models for frequently requested items.				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
DSS02.04 Investigate, diagnose and allocate Incidents. Identify and record incident symptoms, determine possible causes, and allocate for resolution.	BAI07.07	Supplemental support plan	Incident symptoms	Internal
			Problem log	DSS03.01
Activities				
1. Identify and describe relevant symptoms to establish the most probable causes, of the incidents. Reference available knowledge resources (including known errors and problems) to identify possible incident resolutions (temporary workarounds and/or permanent solutions).				
2. If a related problem or known error does not already exist and if the incident satisfies agreed-on criteria for problem registration, log a new problem.				
3. Assign incidents to specialist functions if deeper expertise is needed, and engage the appropriate level of management, where and if needed.				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
DSS02.05 Resolve and recover from Incidents. Document, apply and test the identified solutions or workarounds and perform recovery actions to restore the IT-related service.	APO12.06	Risk-related incident response plans	Incident resolutions	DSS03.04
	DSS03.03	Known error records		
	DSS03.04	Communication of knowledge learned		
Activities				
1. Select and apply the most appropriate incident resolutions (temporary workaround and/or permanent solution).				
2. Record whether workarounds were used for incident resolution.				
3. Perform recovery actions, if required.				
4. Document incident resolution and assess if the resolution can be used as a future knowledge source.				

Beispiel: Basst scho! ...



Quelle: [blog.itil.org/category/cobit/]

COBIT

Verlinkung der Unternehmensziele mit den IT-Zielen

Figure 22—Mapping COBIT 5 Enterprise Goals to IT-related Goals

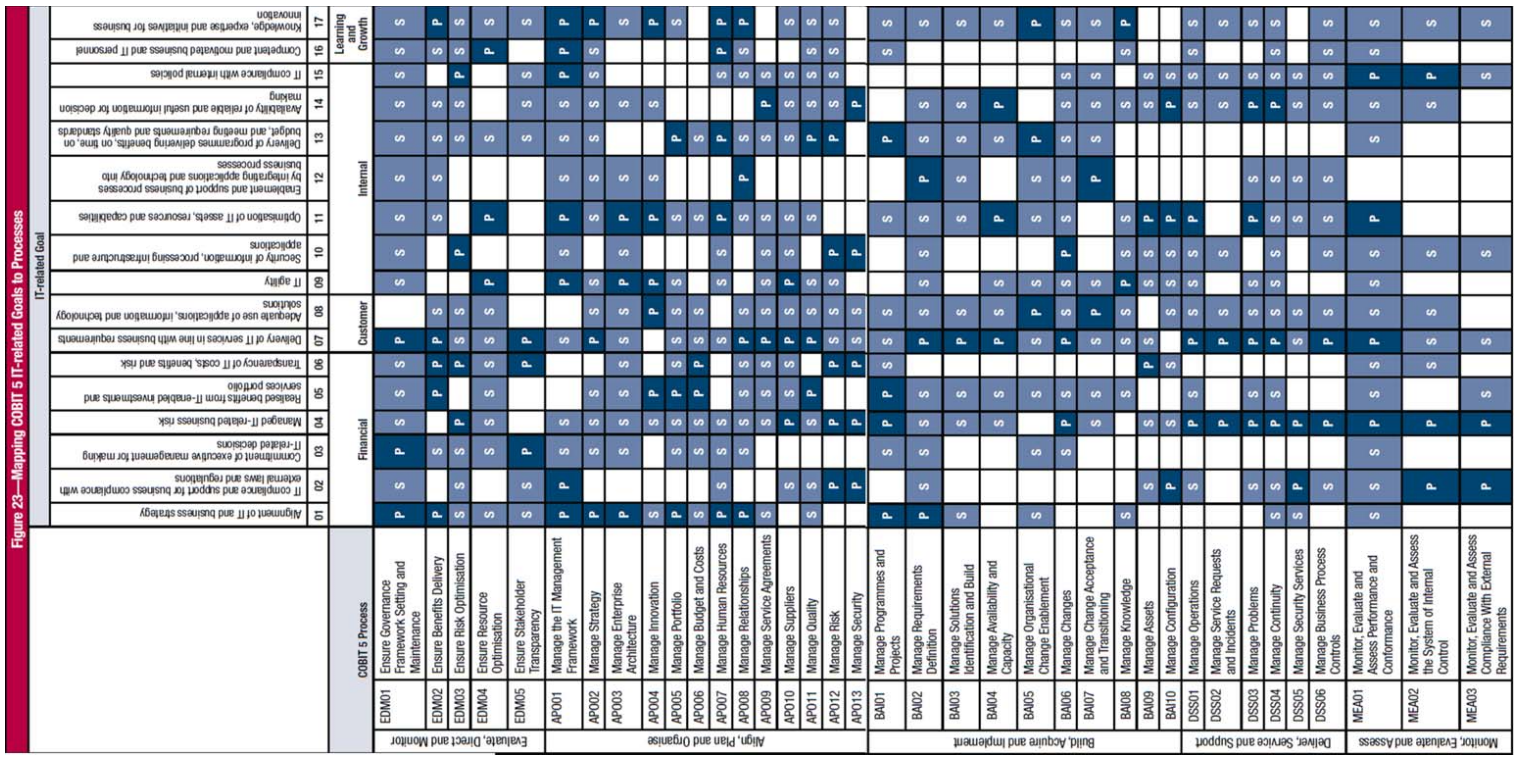
		IT-related Goal	Enterprise Goal																	
			Stakeholder value of business investments	Portfolio of competitive products and services	Managed business risk (safeguarding of assets)	Compliance with external laws and regulations	Financial transparency	Customer-oriented service culture	Business service continuity and availability	Agile responses to a changing business environment	Information-based strategic decision making	Optimisation of service delivery costs	Optimisation of business process functionality	Optimisation of business process costs	Managed business change programmes	Operational and staff productivity	Compliance with internal policies	Skilled and motivated people	Product and business innovation culture
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
			Financial					Customer					Internal					Learning and Growth	
Financial	01	Alignment of IT and business strategy	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	IT compliance and support for business compliance with external laws and regulations			S	P											P		
	03	Commitment of executive management for making IT-related decisions	P	S	S					S	S		S		P			S	S
	04	Managed IT-related business risk			P	S			P	S		P			S		S	S	
	05	Realised benefits from IT-enabled investments and services portfolio	P	P				S		S		S	S	P		S			S
	06	Transparency of IT costs, benefits and risk	S		S		P				S	P		P					
Customer	07	Delivery of IT services in line with business requirements	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Adequate use of applications, information and technology solutions	S	S	S			S	S		S	S	P	S		P		S	S
Internal	09	IT agility	S	P	S			S		P			P		S	S		S	P
	10	Security of information, processing infrastructure and applications			P	P			P								P		
	11	Optimisation of IT assets, resources and capabilities	P	S						S		P	S	P	S	S			S
	12	Enablement and support of business processes by integrating applications and technology into business processes	S	P	S			S		S		S	P	S	S	S			S
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	P	S	S			S				S		S	P				
	14	Availability of reliable and useful information for decision making	S	S	S	S			P		P		S						
	15	IT compliance with internal policies			S	S											P		
Learning and Growth	16	Competent and motivated business and IT personnel	S	S	P			S		S						P		P	S
	17	Knowledge, expertise and initiatives for business innovation	S	P				S		P	S		S		S			S	P

P: primärer Einfluss; S: sekundärer Einfluss

Quelle: [blog.itil.org/category/cobit/]

COBIT

Verlinkung der IT-Ziele mit den Enabler-Zielen



Quelle: [blog.itil.org/category/cobit/]

Anwendung

- Audit-Werkzeug
- keine Risikoanalyse
- wenig geeignet für die Erstellung von Sicherheitshandbüchern (keine detaillierte Beschreibung der zu implementierenden Massnahmen)
- benötigt einen grossen Initialaufwand
- ressourcenintensiv (Vollstudien benötigen $\geq$ 4 Wochen (mehr, falls IT-Verantwortliche nicht zu 100% für das Audit zur Verfügung stehen ...))
- soll regelmässig durchgeführt werden
- oft wird nicht die komplette COBIT durchgeführt, sondern nur einzelne Aspekte.

MEHARI 2010

Méthode Harmonisée d'Analyse de Risques

Methodisch einfache Risikoanalyse und Hilfe zur Erstellung von Sicherheitskonzepten

Methodischer Ansatz

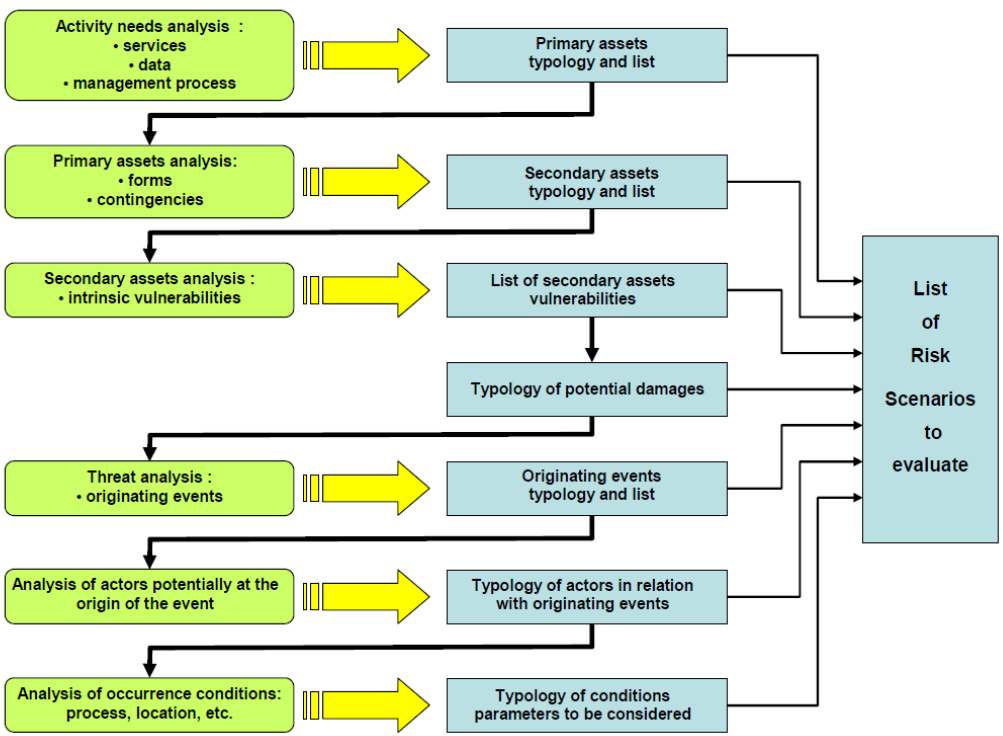
- Entwickler: CLUSIF [Club de la Sécurité de l'Information Français]
- Risk Assessment
  - Identifizierung von Gefahren und Risiken
  - Risiko-Berechnung
  - Risikobeurteilung
- Konform mit ISO 2700x
- Mischung aus
  - tabellengestützter Ansatz/Fragebögen
  - „Wissenskatalog"
  - experteneinschätzung
- Tabellen (Open soruce): [download CLUSIF]

Quelle: Alle Angaben zu MEHARI aus [3]

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering
INE Institut für Nachhaltige Entwicklung

Risikoidentifikation

- Arten primärer Assets ⇒ Tab. A1
- Arten sekundärer Assets ⇒ Tab. A2
- Eigen-Vulnerabilities sekundärer Assets ⇒ Tab. B
- Arten auslösender Ereignisse ⇒ Tab. C1
- Akteure ⇒ Tab. C2



Klassifizierung der primären Assets (A1)

Data and information assets		A	I	C
Data and information				
D01	Data files and data bases accessed by applications			
D02	Shared office files and data			
D03	Personal office files (on user work stations and equipments)			
D04	Written or printed information and data kept by users and personal archives			
D05	Listings or printed documents			
D06	Exchanged messages, screen views, data individually sensitive			
D07	electronic mailing			
D08	(Post) Mails and faxes			
D09	Patrimonial archives or documents used as proofs			
D10	IT related Archives			
D11	Data and information published on public or internal sites			
Service assets		**A**	**I**	**C**
General Services				
G01	User workspace and environment			
G02	Telecommunication Services (voice, fax, audio & videoconferencing, etc.)			
IT and Networking Services				
R01	Extended Network Service			
R02	Local Area Network Service			
S01	Services provided by applications			
S02	Shared Office Services (servers, document management, shared printers, etc.)			
S03	Users' disposal of Equipments (workstations, local printers, peripherals, specific interfaces, etc.) **Nota : Applies to a massive loss of these services, not for one or few users.**			
S04	Common Services, working environment: messaging, archiving, print, editing, etc.			
S05	Web editing Service (internal or public)			
Management process type of assets		**E**		
Management Processes for compliance to law or regulations				
C01	Compliance to law or regulations relative to personal information protection			
C02	Compliance to law or regulations relative to financial communication			
C03	Compliance to law or regulations relative to digital accounting control			
C04	Compliance to law or regulations relative to intellectual property			
C05	Compliance to law or regulations relative to the protection information systems			
C06	Compliance to law or regulations relative to people safety and protection of environment			

Klassifizierung der sekundären Assets (A2)

SECONDARY ASSET TYPES
Asset category: Services
Service support hardware equipment
Software configurations
Software support media
Accounts and means necessary to access the service
Security services associated with the service
Ancillary means necessary for the service
Premises
Personnel and service providers necessary for the service (internal and external)

Asset category: Data
Logical entities: files or databases
Logical entities: transiting data packets or messages
Physical entities: media and devices
Means for accessing data: keys and other means, physical or logical, required to access the data

Asset category: Management processes
Internal guidelines and procedures (organizational tools)
Physical resources necessary for management processes
Personnel and service providers necessary for management processes

Eigen-Vulnerabilities sekundärer Assets (B)

List of intrinsic vulnerabilities			
Type of supporting asset	***Type of damage***	***Type of vulnerability***	***Criteria AICE***
Category: Service			
Hardware (Equipment)	Destruction	Possibility of destruction of equipment	A
	Failure	Possibility of failure of equipment	A
	Not operable	Possibility of non operable equipment	A
Software Configuration	Alteration	Possibility of alteration of software configurations (software and parameters)	A and I
	Failure	Possibility of software failure (bug)	A
	Erasure	Possibility of erasure of software configurations	A
	Unauthorized use	Possibility of denial to use (due to lack of license)	I
	Pollution	Possibility of pollution of software configurations	I
	Disclosure of software	Possibility of disclosure of a software file	A
		Possibility of destruction of media containing	

- Kriterien: C: Confidentiality; I: Integrity; A: Availability; E: Efficiency
- Kategorien: Service, Data, Management Process

Auslösende Ereignisse Assets (C1)

Table of events : types of events and natural exposure

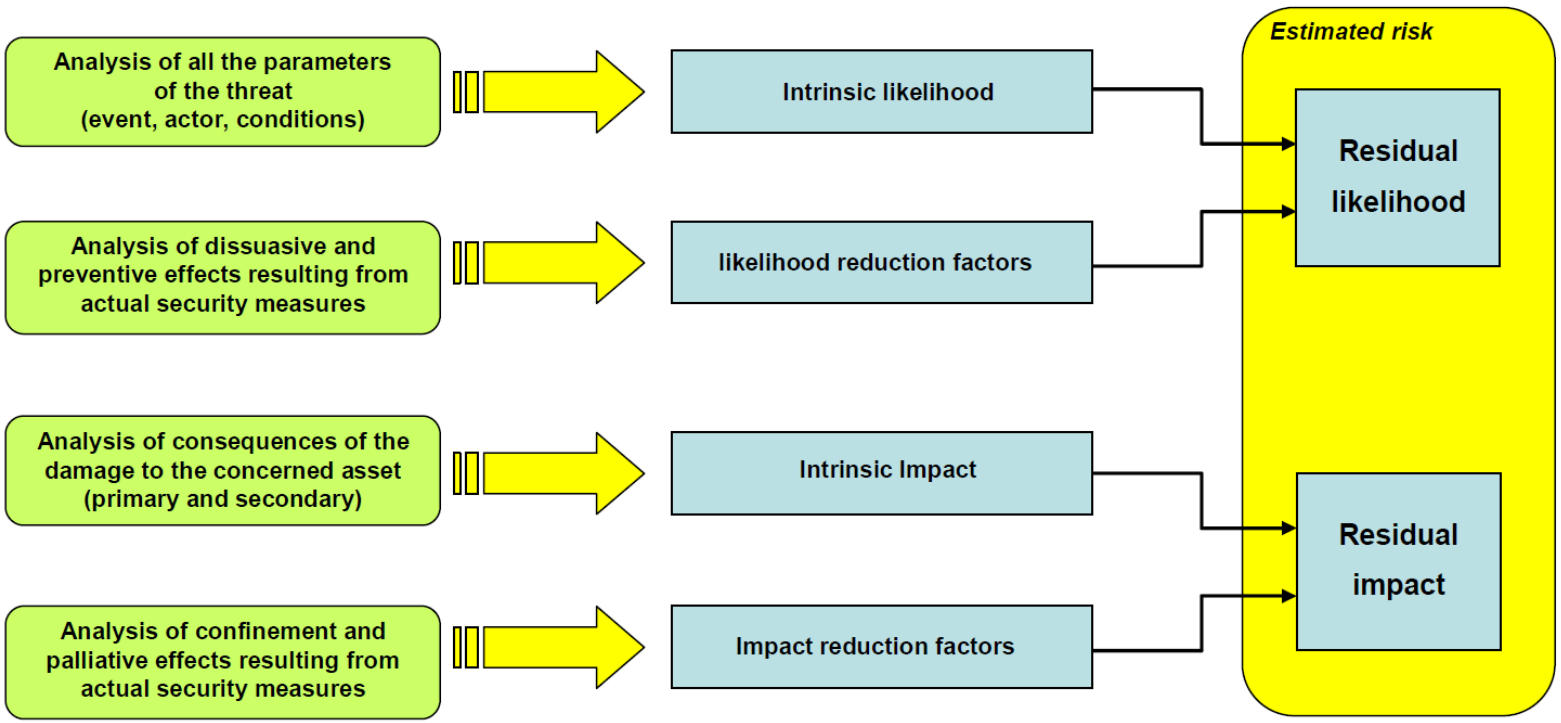
Family type	*Code type*	*Event description*	*Code*
Absence of personnel due to an accident	AB.P	Absence of personnel from partner	AB.P.Pop
		Absence of internal personnel	AB.P.Per
Accidental absence or unavailability of service	AB.S	Absence of service : Power supply	AB.S.Ene
		Absence of service : Air conditioning	AB.S.Cli
		Absence of service : Impossibility to have access to the premises	AB.S.Loc
		Absence or impossibility of application software maintenance	AB.S.Maa
		Absence or impossibility of information system maintenance	AB.S.Mae
Environmental serious accident	AC.E	Lightning	AC.E.Fou
		Fire	AC.E.Ine
		Flooding	AC.E.Ino
Hardware accident	AC.M	Equipment breakdown	AC.M.Equ
		Accessory equipment breakdown	AC.M.Ser
Voluntary absence of personnel	AV.P	Social conflict with strike	AV.P.Gre
Conceptual error	ER.L	Software blocking or malfunction due to a design or programming error (in-house software)	ER.L.Lin
Hardware error or behavioural error by personnel	ER.P	Lost or forgotten document or media	ER.P.Poo
		Error of operation or non compliance of a procedure	ER.P.Pro
		Typing or data entry error	ER.P.Pra
Incident due to environment	IC.E	Damage due to ageing (of equipment)	IC.E.Age
		Water damage	IC.E.De
		Electrical boosting or over load	IC.E.Sc
		Pollution damage	IC.E.Pol
Logical or functional incident	IF.L	Production incident	IF.L.Exp
		Software blocking or malfunction (information system or software package)	IF.L.Lap
		Saturation due to an external cause (worm)	IF.L.Ver
		Virus	IF.L.Vir
Malevolent action (logical or functional)	MA.L	Deliberate blocking of accounts	MA.L.Blo
		Deliberate erasure or massive pollution of system configurations	MA.L.Cfg
		Deliberate erasure of files, data bases or media	MA.L.Del
		Electromagnetic pick up	MA.L.Ele
		Deliberate corruption of data or functions	MA.L.Fal
		Forging of messages or data	MA.L.Fau
		Fraudulent replay of transaction	MA.L.Rej
		Deliberate saturation of IT equipments or networks	MA.L.Sam
		Deliberate total erasure of files and backups	MA.L.Tot
		Diversion of files or data (tele-load or copy)	MA.L.Vol
Malevolent action (physical)	MA.P	Tampering or falsification of equipment	MA.P.Fal
		Terrorism	MA.P.Ter
		Vandalism or hooliganism	MA.P.Van
		Theft of physical asset	MA.P.Vol
Non compliance to procedures	PR.N	Inadequate procedures	PR.N.Apl
		Procedures not applied due to lack of resource or means	PR.N.Naa
		Procedures not applied due to ignorance	PR.N.Nam
		Procedures not applied deliberately	PR.N.Nav

Akteure (C2)

Category	***Typology***
Member of personnel, user of IT system	authorized user legitimately
	authorized user illegitimately
Personnel with specific rights	member of operations personnel
	member of development team
	member of maintenance personnel
	member of service personnel (upkeep, g security, etc.)
Personnel authorized within the establishment	member of personnel (internal or not) (permanent or not)
	Visitor
Personnel not authorized within the establishment	third party not authorized
	Vandal or terrorist

Risk Assessment

- Auswirkungslevels C, ohne Sicherheitsmassnahmen $\Rightarrow$ Tab. D1
- Häufigkeitslevels F, ohne Sicherheitsmassnahmen $\Rightarrow$ Tab. D2
- Einfluss von Sicherheitsmassnahmen auf F und C $\Rightarrow$ Tab. E1, E2



Schwerelevels *C* (D1)

Scale of impact

Level 4: Vital

At this level, the impact is very serious, and even the existence and survival of the entity (or at least one of its main activities) is in danger.

Should the organization survive such a malfunction, there would be serious and durable consequences.

Level 3: Very Serious

The impact is considered very serious at the level of the entity, although its future would not be at risk.

In financial terms, this would have a seriously negative impact on the profits for the period, although there would not be a massive pull-out by shareholders.

In terms of public image, this level of malfunction often damages the organization's reputation to such an extent that it would take several months to restore it, even if the financial impact cannot be precisely evaluated.

Accidents that lead to months of organizational disorder for an enterprise would also be evaluated at this level.

Level 2: Serious

Malfunctions at this level would have a clear impact on the entity's operations, results or image, but are globally manageable.

Level 1: Not significant

At this level, any resulting damage would have no significant impact on the results or image of the entity, even if some staff members were deeply involved in re-establishing the original status

Häufigkeitslevels *F* (D2)

Scale of likelihood

Level 4: Very likely

At this level, it is wise to consider that the scenario is likely to happen almost certainly and probably in the short term.

When the risk occurs, nobody shall be surprised.

Level 3: Likely

This corresponds to scenarios that are bound to happen in the more or less short term.

One may still hope they will not happen but it is rather optimistic.

The environment and context of the enterprise are such that, if nothing is done to avoid it, the given scenario is bound to happen in the more or less short term.

Level 2: Unlikely

It is reasonable to think that these scenarios should not occur.

The past experience shows that they have not occurred.

However they are to be listed as not unrealistic.

Level 1: Very unlikely

At this level, the potentiality of the risk appears to be very low.

But these scenarios are not strictly impossible as there is always a tiny probability of occurrence

Einfluss abschreckender & vorbeugender Massnahmen auf *F* (E1)

Efficiency of dissuasion measures

Level 4: *The effect of dissuasive measures is very high.*
The potential attacker can logically consider that he or she should abandon any idea of performing the action. They should realize that they will certainly be identified, and that the resulting punishment will well outweigh any potential gain.

Level 3: *The effect of dissuasive measures is high.*
The potential attacker can logically consider that he or she runs a high risk. They should realize that they will undoubtedly be identified, and that punishment will be serious.

Level 2: *The effect of dissuasive measures is medium.*
The potential attacker can logically consider that he or she runs only a small risk. In any case, any potential personal prejudice will be supportable.

Level 1: *The effect of dissuasive measures is low or nil.*
The potential attacker can logically consider that he or she runs no personal risk. They can consider that they will not be identified, or will have the possibility of using strong arguments to refute any accusations concerning actions performed, or that any punishment will be very light.

Efficiency of prevention measures.

Level 4: *The effect of the preventive measures is very high.*
Only a few determined experts, with exceptional means, could succeed.
Only the conjunction of very rare or extremely exceptional circumstances would permit this scenario to happen.

Level 3: *The effect of the preventive measures is high.*
Only a specialist, or a professional with special tools or means, or a group of professionals in collusion and using their collective means and tools could succeed.
This is usually the result of the conjunction of rare or exceptional circumstances.

Level 2: *The effect of the preventive measures is medium.*
A professional can set off the scenario, without the need for special means or tools outside of those available in the profession.
Rare natural circumstances can produce the same result.

Level 1: *The effect of the preventive measures is low or nil.*
Any person in the organization, or close to it, or even someone, who knows something about it, is capable of setting this scenario in motion, with the means at their disposal (or easy to obtain).
Perfectly ordinary circumstances can be the cause of this scenario (misuse, error, ordinary unfavorable conditions).

Einfluss schützender/einschränkender & lindernder Massnahmen auf *C* (E2)

Efficiency of the protective or confinement measures

Level 4: *The measures have a very strong effect.*
Direct consequences will be very limited. The residual impact will be low or even not significant.

Level 3: *The confinement measures have an important effect to limiting the direct consequences.*
The limits imposed to the scenario will decrease the consequences and the event will be rapidly detected, with immediate reaction.
The protective measures that are used will have a real influence on the direct impact, which remains limited in scope, and manageable.

Level 2: *The effect of the confinement and the limitation of the direct consequences is medium.*
The damage may be feebly limited in its direct consequences if it is detected,
but the time to detect and react will be long.
The protective measures that are used have a real influence on the result,
but the direct consequences are still very big.

Level 1: *The effects of the confinement and the limitation of the direct consequences are very low or nil.*
Either the damage and its direct consequences cannot be limited, because of the delay of detection
or it will not be detected for some time.
The measures will only have a very restricted influence on the level of the direct consequences.

Efficiency of the Palliative measures

Level 4: *The effects of the limitation of the indirect consequences are very high indeed.*
Normal operations continue without any noticeable interruption.

Level 3: *The effects of the limitation of the indirect consequences are high.*
The palliative measures have not only been finely planned and organized, but also tested and validated.
The time to re-establish normal operations can be precisely estimated or known,
and is such that it will measurably reduce the gravity seriousness of the indirect consequences of the scenario.

Level 2: *The effects of the limitation of the indirect consequences are medium.*
The relief or palliative solutions have been broadly planned, but the fine detail is missing.
It can be considered that, due to the lack of detail, there will be a corresponding lack of efficiency of the palliative measures.
The time to re-establish normal operations cannot be precisely predicted, or will not fundamentally change the nature of the damage caused.

Level 1: *The effects of the limitation of the indirect consequences are very low or nil.*
Either totally improvised measures are used, or it is considered that their effect will be low.

Risk Evaluation

- Bestimmen der Rest-Risiken (s.o.)
- Bestimmung des Häufigkeitslevels $F \Rightarrow$ D2
- Effizienz der abschreckenden Massnahme DISS $\Rightarrow$ E1
- Effizienz der vorbeugender Massnahmen PREV $\Rightarrow$ E1

$\Rightarrow$ Schwere-Grad für Likelihood L aus Grid F1

- Bestimmung des Schwerelevels $C \Rightarrow$ D1
- Effizienz der Schutz-Massnahme CONF $\Rightarrow$ E2
- Effizienz der minimierenden Massnahme PALL $\Rightarrow$ E2

$\Rightarrow$ Schwere-Grad für Impact I aus Grid F2

$\Rightarrow$ Eintragen der Schweregrade für L und I Risiko-Matrix $\Rightarrow$ Abb. F3

Bewertung des Schweregrades für Likelihood L (F1)

Grids of evaluation of STATUS-P

1. Scenarios resulting from an Accident

DISS	EXPO = 1	EXPO = 2	EXPO = 3	EXPO = 4
1	1 1 1 1	2 2 2 1	3 3 2 1	4 4 2 1
	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4
	P R E V	P R E V	P R E V	P R E V

2. Scenarios resulting from an Error

DISS	EXPO = 1	EXPO = 2	EXPO = 3	EXPO = 4
1	1 1 1 1	2 2 2 1	3 3 2 1	4 4 2 1
	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4
	P R E V	P R E V	P R E V	P R E V

3. Scenarios resulting from a Voluntary action

DISS	EXPO = 1	EXPO = 2	EXPO = 3	EXPO = 4
4	1 1 1 1	1 1 1 1	2 2 1 1	2 2 2 1
3	1 1 1 1	2 2 1 1	2 2 1 1	3 3 2 2
2	1 1 1 1	2 2 2 1	3 3 2 1	4 4 3 2
1	1 1 1 1	2 2 2 1	3 3 2 1	4 4 3 2
	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4
	P R E V	P R E V	P R E V	P R E V

Bewertung des Schweregrades für Impact I (F2)

Grids of of evaluation of STATUS-I

The non evolutionary scenarios are represented on the nc line

1. Scenarios affecting Availability

C	II = 1	II = 2	II = 3	II = 4
4	1 1 1 1	2 2 1 1	2 2 1 1	2 2 2 1
3	1 1 1 1	2 2 1 1	3 2 2 1	3 3 2 1
2	1 1 1 1	2 2 2 1	3 3 2 1	4 3 2 1
1	1 1 1 1	2 2 2 1	3 3 2 1	4 3 2 1
nc	1 1 1 1	2 2 2 1	3 3 2 1	4 3 2 1
	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4
	P A L L	P A L L	P A L L	P A L L

2. Scenarios affecting Integrity

C	II = 1	II = 2	II = 3	II = 4
4	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1
3	1 1 1 1	2 2 1 1	2 2 1 1	2 2 2 1
2	1 1 1 1	2 2 2 1	3 3 2 1	3 3 2 1
1	1 1 1 1	2 2 2 1	3 3 2 1	4 3 2 1
nc	1 1 1 1	2 2 2 2	3 3 2 2	4 4 4 4
	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4
	P A L L	P A L L	P A L L	P A L L

3. Scenarios affecting Confidentiality

C	II = 1	II = 2	II = 3	II = 4
4	1	2	2	2
3	1	2	2	2
2	1	2	3	3
1	1	2	3	4
nc	1	2	3	4
	1	1	1	1
	P A L L	P A L L	P A L L	P A L L

4. Type L (limitable) scenarios

C	II = 1	II = 2	II = 3	II = 4
4	1	1	1	1
3	1	2	2	2
2	1	2	3	3
1	1	2	3	4
	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4
	P A L L	P A L L	P A L L	P A L L

Risikomatrix (F3)

I = 4	S = 2	S = 3	**S = 4**	**S = 4**
I = 3	S = 2	S = 3	S = 3	**S = 4**
I = 2	S = 1	S = 2	S = 2	S = 3
I = 1	S = 1	S = 1	S = 1	S = 2
	L = 1	L = 2	L = 3	L = 4

Beispiel (für Szenario Availability)

Aus Liste Restrisiko: Hardware-Ausfall Server xy („Accident"; hat Einfluss auf „Availability"; es gibt Massnahmen zur Risikoreduktion)

- Häufigkeitslevel F nach D2: Level 3 (likely) $\widehat{=}$ Belastungs-Indikator $EXPO = 3$
- Effizienz abschreckender Massnahmen DISS nach E1: Level 1 (unbedeutend, da zufälliger Ausfall)
- Effizienz vorbeugender Massnahmen PREV nach E1: Level 3 (hoch, regelm. Wartung)

$\Rightarrow$ Grad für Likelihood L aus Grid F1: $L = 2$

- Schwerelevel C nach D1: Level 3 (sehr stark) $\widehat{=}$ Impact-Indikator $II = 3$
- Effizienz der Schutz-Massnahmen CONF nach E2: Level 4 (sehr hoch)
- Effizienz minimierender Massnahmen nach E2 PALL: Level 3 (hoch)

$\Rightarrow$ Grad für Impact aus Grid F2: $I = 1$

$\rightrightarrows$ Eintrag in die Risiko-Matrix F2: Aus Koordinaten $L = 2$ und $I = 1$ folgt Schweregrad $S = 1$, d.h. Risiko akzeptabel (grünes Feld)

Anmerkungen zu MEHARI

- Framework (und Tool), um Risikoanalysen in der IT durchzuführen
- Checklistenverfahren und damit wenig flexibel auf neue Gefahren und Risiken (Einsatzgebiet eher im Bereich „Überprüfung der Grundsicherheit bzw. des Grundschutzes“
- liefert eine breite Wissensbasis.
- Die Basis wird ergänzt durch eine Spezifikation mit Bezug auf IT Security Dienste mit Qualitäts-Kriterien hierfür und Massnahmen (siehe [3])
- Eignet sich u. U. nicht für Start-up-Unternehmen, da viele prozess noch nicht definiert sind
- Eignet sich nicht, wenn Prozesse ausgelagert sind, z.B. die Server-Infrastruktur eines Unternehmens)

IT-Grundschutzkataloge

Erreichen eines Sicherheitsniveaus, das für den niederen bis mittleren Schutzbedarf angemessen und ausreichend ist.

Anmerkung

Die Kataloge sind vollständig dokumentiert: [Bundesamt für Sicherheit und Informationstechnik BSI]

Ansatz

- Die Methode ist als Baukasten konzipiert, wobei ein IT-Verbund in 5 Schichten mit zugehörigen Bausteinen (B) strukturiert ist
  - Schicht 1: Bausteine B1.x: Übergreifende Aspekte
  - Schicht 2: Bausteine B2.x: Infrastruktur
  - Schicht 3: Bausteine B3.x: IT-Systeme
  - Schicht 4: Bausteine B4.x: Netze
  - Schicht 5: Bausteine B5.x: Anwendungen
- Zu den Bausteinen gibt es
  - Gefährdungskataloge (G)
  - Massnahmenkataloge (M)
- Gibt für jeden Baustein (B) vor, welche Gefährdungen (G) und Massnahmen (M) relevant sind.

Bausteine B1.x: Übergreifende Aspekte

0 IT-Sicherheitsmanagement
1 Organisation
2 Personal
3 Notfallvorsorge-Konzept
4 Datensicherungskonzept
5 Datenschutz

...

16 Anforderungsmanagement

Gefährdungskataloge G

G1 höhere Gewalt

G1.1 Personalausfall

G1.2 Ausfall von IT-Systemen:

Der Ausfall einer Komponente eines IT-Systems kann zu einem Ausfall des gesamten IT-Betriebs und damit dem Ausfall wichtiger Geschäftsprozesse führen. Insbesondere zentrale Komponenten eines IT-Systems sind geeignet, solche Ausfälle herbeizuführen, z. B. LAN-Server, Netzkoppelelemente. Auch der Ausfall von einzelnen Komponenten der technischen Infrastruktur, beispielsweise Klima- oder Stromversorgungseinrichtungen, kann zu einem Ausfall des gesamten Informationsverbunds IT-Systems beitragen.
Ursache für den Ausfall eines IT-Systems ist nicht immer technisches Versagen (z. B. G 4.1 Ausfall der Stromversorgung). Ausfälle lassen sich auch oft auf menschliches Fehlverhalten (z. B. G 3.2 Fahrlässige Zerstörung von Gerät oder Daten) oder vorsätzliche Handlungen (z. B. G 5.4 Diebstahl , G 5.102 Sabotage) zurückführen. Auch mangelnde Wartung, beispielsweise durch Ausfall des Wartungspersonals, kann zu technischem Versagen führen. Auch durch höhere Gewalt (z. B. Feuer, Blitzschlag, Chemieunfall) können Schäden eintreten, allerdings sind diese Schäden meist um ein Vielfaches höher.
Werden auf einem IT-System zeitkritische Anwendungen betrieben, sind die Folgeschäden nach einem Systemausfall entsprechend hoch, wenn es keine Ausweichmöglichkeiten gibt.
Beispiele: *dots*

...

G2 organisatorische Mängel

G3 menschliche Fehlhandlungen

G4 technisches Versagen

G5 vorsätzliche Handlungen

Massnahmenkataloge M

- M1 Infrastruktur
  - M1.1 Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
  - M1.2 Regelungen für Zutritt zu Verteilern
  - ...
- M2 Organisation
- M3 Personal
- M4 Hardware und Software
- M5 Kommunikation
- M6 Notfallvorsorge

Hilfsmittel

- Checklisten und Formulare
- Muster und Beispiele
- IT-Grundschutz-Beispielprofile
- Bausteine
- Dokumentationen und Studien
- Informationen externer Anwender
- Entfallene Bausteine
- Archiv

Anwendung

- Unterstützung bei der Erarbeitung (physikalischer) IT-Security-Konzepte
- keine Bedrohungs- und Risikoanalyse (soll diese eher vermeiden helfen)
- fehlender konzeptioneller Überbau, z.B. durch Unternehmensziele

MELANI: Melde- und Analysestelle Informationssicherung

Organisation

Zusammenarbeit von Partnern, die im Umfeld der Sicherheit von Computersystemen und des Internets sowie des Schutzes der schweizerischen kritischen Infrastrukturen tätig sind. Es sind dies:

- GovCERT.ch → siehe [FIRST: Forum of Incident Response and Security Teams]
- Nachrichtendienst des Bundes [NDB]
- Informatiksteuerungsorgan des Bundes [ISB]

Aufgaben und Leistungen

- Schweizer Meldestelle
- Umfeld: Sicherheit von Computersystemen, Internet, Schutz der schweizerischen kritischen Infrastrukturen
- richtet sich an private Computer- und Internetbenutzer, sowie kleinere und mittlere Unternehmen (KMU)
- publiziert halbjährliche Berichte „Informationssicherung: Lage in der Schweiz und international
- nennt allgemeine Massnahmen zur IT-Security
- Links: [MELANI]

Informationsquellen

MELANI: Halbjahresbericht 2013/2 (Auszug)

- **Weitere Enthüllungen zu NSA und GCHQ**
  Auch im zweiten Halbjahr 2013 waren die diversen veröffentlichten Aktivitäten basierend auf den Dokumenten von Edward Snowden rund um die US-National Security Agency (NSA) und das Britische General Communication Headquarter (GCHQ) ein grosses Thema. Im zweiten Halbjahr vervollständigte sich das Bild einer flächendeckenden und vollumfassenden Datenerfassung durch diese Nachrichtendienste. Die Erkenntnisse zeigen die Probleme auf, die eine solch transnationale Einrichtung wie das Internet mit sich bringt, an der jedes Individuum, jeder Staat so teilhaben kann und vorgehen darf, wie es ihm gerade beliebt und die nationalen Gesetze es zulassen, ohne dabei auf die globalen Auswirkungen Rücksicht nehmen zu müssen.
  ▶ Aktuelle Lage International: Kapitel 4.1
  ▶ Tendenzen / Ausblick: Kapitel 5.1
- **Bitcoin: der Erfolg und sein Preis**
  Bitcoin ist eine dezentrale digitale Währung, das heisst sie hängt von keiner zentralen Ausgabestelle ab. Dadurch unterscheidet sie sich nicht nur von den traditionellen, sondern auch von anderen digitalen Währungen. Mit zunehmender Popularität von Bitcoin stellen sich Fragen insbesondere in Bezug auf das Sicherheitsniveau aber auch den Rechtsstatus und die Regulierung dieser Devisen.
  ▶ Tendenzen / Ausblick: Kapitel 5.2
- **Ransomware auf dem Vormarsch**
  Bei Ransomware (auf deutsch erpresserische Schadsoftware) sehr verbreitet, sind die Sperrtrojaner, welche auf infizierten Computern eine Meldung anzeigen, die scheinbar von einer Polizeibehörde stammt. Weit schwerwiegender ist eine Infektion mit der Schadsoftware Cryptolocker, welche in der Schweiz das erste Mal im November 2013 beobachtet worden ist. Hier werden alle Daten, die sich auf der Festplatte und auf allen anderen angeschlossenen Datenträgern befinden, verschlüsselt und sind damit für das Opfer nicht mehr zugänglich.
  ▶ Aktuelle Lage Schweiz: Kapitel 3.1
- **Grosse Datendiebstähle**
  Wieder sind Datendiebstähle bekannt geworden, welche mehrere Millionen Datensätze betroffen haben. Bei Adobe waren nach eigenen Angaben 38 Millionen Kundendaten, Passwörtern und Kreditkartendaten betroffen. Die Ladenkette Target war ebenfalls Opfer eines grossen Datendiebstahls. Laut den publizierten Informationen wurden 40 Millionen Kreditkarten- und 70 Millionen Kundendaten gestohlen.
  ▶ Aktuelle Lage International: Kapitel 4.3, Kapitel 4.4
- **Industrielle und private Kontrollsysteme – Immer mehr Systeme am Internet**
  Es ist mittlerweile relativ einfach und günstig, Systeme mit Fernabfrage- und -steuerungsfunktion zu beziehen oder eine bestehende Anlage mit einer Kommunikationsschnittstelle nachzurüsten. Entsprechend ist neben Funktion und Benutzerfreundlichkeit einer Fernzugangslösung auch dem Schutz vor unbefugten Manipulationen Beachtung zu schenken. MELANI hat hierzu im Oktober 2013 eine Checkliste zum Schutz von industriellen Kontrollsystemen publiziert.
  ▶ Aktuelle Lage International: Kapitel 4.7

Quelle: [MELANI Dokumentation]

Einsatz bei IT-Security-Analysen

- MELANI-Dokumentationen ersetzen keine (Risiko-) Analysen
- aber: helfen, Analysen in Unternehmen aktuell zu halten und auf neuere Bedrohungen zur reagieren
- Berücksichtigung des Schweizer Umfeldes

US-CERT: US Computer Emergency Readiness Team

„The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. US-CERT strives to be a trusted global leader in cybersecurity - collaborative, agile, and responsive in a dynamic and complex environment".

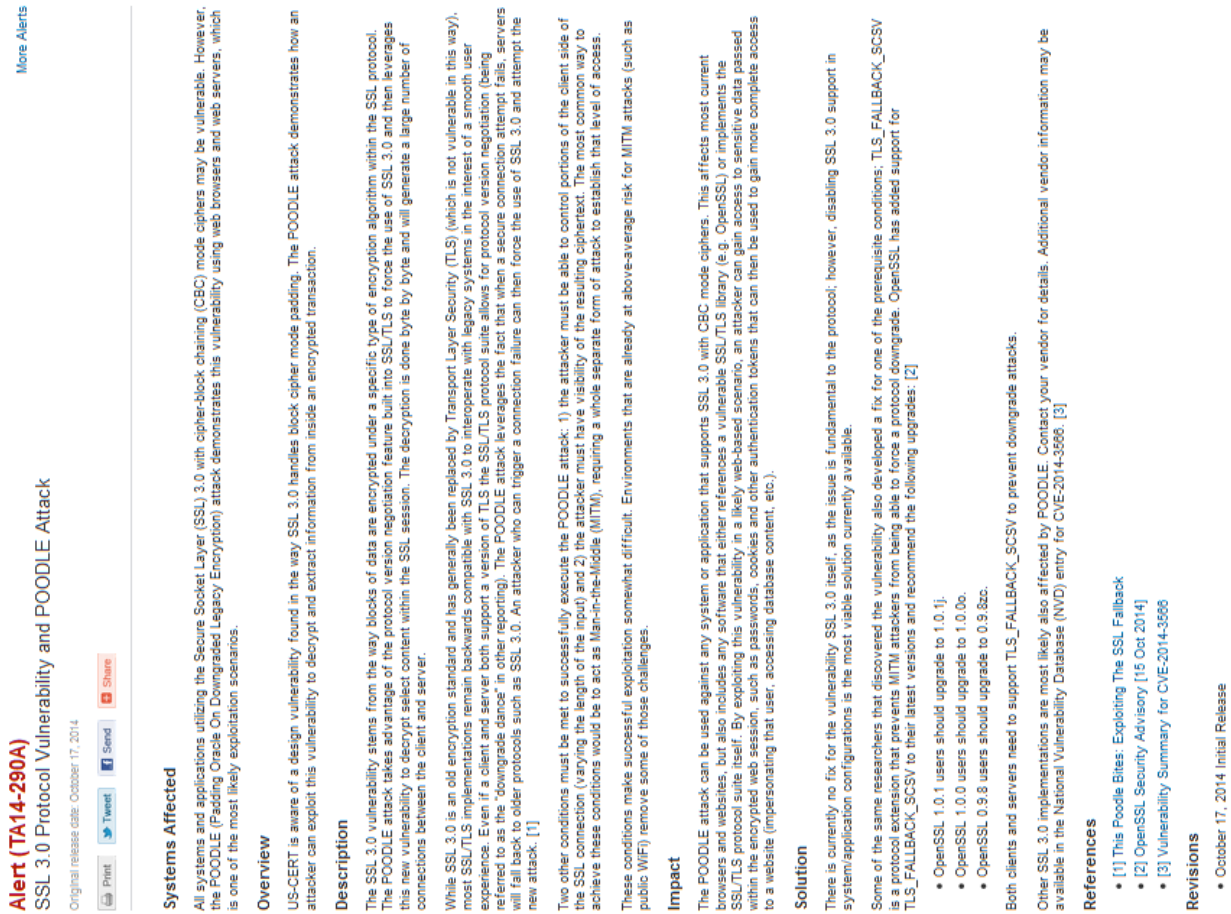
National Cyber Awareness System

- **Current Activity:**...updates provide timely information on security risks to help you better protect your systems from malware campaigns and mitigate against new software vulnerabilities. Current Activity is updated frequently and typically contains less detail than Alerts.
- **Alerts** warn about vulnerabilities, incidents, and other security issues that pose a significant risk. Alerts contain more detailed information and are not issued as frequently as Current Activity updates.
- **Bulletins** provide weekly summaries of new vulnerabilities. Patch information is provided when available.
- **Tips** provide advice about common security issues for the general public.

Quelle: [CERT-alerts and tips]

US-CERT: Alert (TA14-290A)

SSL 3.0 Protocol Vulnerability and POODLE Attack



More Alerts

Alert (TA14-290A)
SSL 3.0 Protocol Vulnerability and POODLE Attack

Original release date: October 17, 2014

Print Tweet Send Share

Systems Affected

All systems and applications utilizing the Secure Socket Layer (SSL) 3.0 with cipher-block chaining (CBC) mode ciphers may be vulnerable. However, the POODLE (Padding Oracle On Downgraded Legacy Encryption) attack demonstrates this vulnerability using web browsers and web servers, which is one of the most likely exploitation scenarios.

Overview

US-CERT is aware of a design vulnerability found in the way SSL 3.0 handles block cipher mode padding. The POODLE attack demonstrates how an attacker can exploit this vulnerability to decrypt and extract information from inside an encrypted transaction.

Description

The SSL 3.0 vulnerability stems from the way blocks of data are encrypted under a specific type of encryption algorithm within the SSL protocol. The POODLE attack takes advantage of the protocol version negotiation feature built into SSL/TLS to force the use of SSL 3.0 and then leverages this new vulnerability to decrypt select content within the SSL session. The decryption is done byte by byte and will generate a large number of connections between the client and server.

While SSL 3.0 is an old encryption standard and has generally been replaced by Transport Layer Security (TLS) (which is not vulnerable in this way), most SSL/TLS implementations remain backwards compatible with SSL 3.0 to interoperate with legacy systems in the interest of a smooth user experience. Even if a client and server both support a version of TLS the SSL/TLS protocol suite allows for protocol version negotiation (being referred to as the "downgrade dance" in other reporting). The POODLE attack leverages the fact that when a secure connection attempt fails, servers will fall back to older protocols such as SSL 3.0. An attacker who can trigger a connection failure can then force the use of SSL 3.0 and attempt the new attack. [1]

Two other conditions must be met to successfully execute the POODLE attack: 1) the attacker must be able to control portions of the client side of the SSL connection (varying the length of the input) and 2) the attacker must have visibility of the resulting ciphertext. The most common way to achieve these conditions would be to act as Man-in-the-Middle (MITM), requiring a whole separate form of attack to establish that level of access.

These conditions make successful exploitation somewhat difficult. Environments that are already at above-average risk for MITM attacks (such as public WiFi) remove some of those challenges.

Impact

The POODLE attack can be used against any system or application that supports SSL 3.0 with CBC mode ciphers. This affects most current browsers and websites, but also includes any software that either references a vulnerable SSL/TLS library (e.g. OpenSSL) or implements the SSL/TLS protocol suite itself. By exploiting this vulnerability in a likely web-based scenario, an attacker can gain access to sensitive data passed within the encrypted web session, such as passwords, cookies and other authentication tokens that can then be used to gain more complete access to a website (impersonating that user, accessing database content, etc.).

Solution

There is currently no fix for the vulnerability SSL 3.0 itself, as the issue is fundamental to the protocol; however, disabling SSL 3.0 support in system/application configurations is the most viable solution currently available.

Some of the same researchers that discovered the vulnerability also developed a fix for one of the prerequisite conditions: TLS_FALLBACK_SCSV is a protocol extension that prevents MITM attackers from being able to force a protocol downgrade. OpenSSL has added support for TLS_FALLBACK_SCSV to their latest versions and recommend the following upgrades: [2]

- OpenSSL 1.0.1 users should upgrade to 1.0.1j.
- OpenSSL 1.0.0 users should upgrade to 1.0.0o.
- OpenSSL 0.9.8 users should upgrade to 0.9.8zc.

Both clients and servers need to support TLS_FALLBACK_SCSV to prevent downgrade attacks.

Other SSL 3.0 implementations are most likely also affected by POODLE. Contact your vendor for details. Additional vendor information may be available in the National Vulnerability Database (NVD) entry for CVE-2014-3566. [3]

References

- [1] This Poodle Bites: Exploiting The SSL Fallback
- [2] OpenSSL Security Advisory [15 Oct 2014]
- [3] Vulnerability Summary for CVE-2014-3566

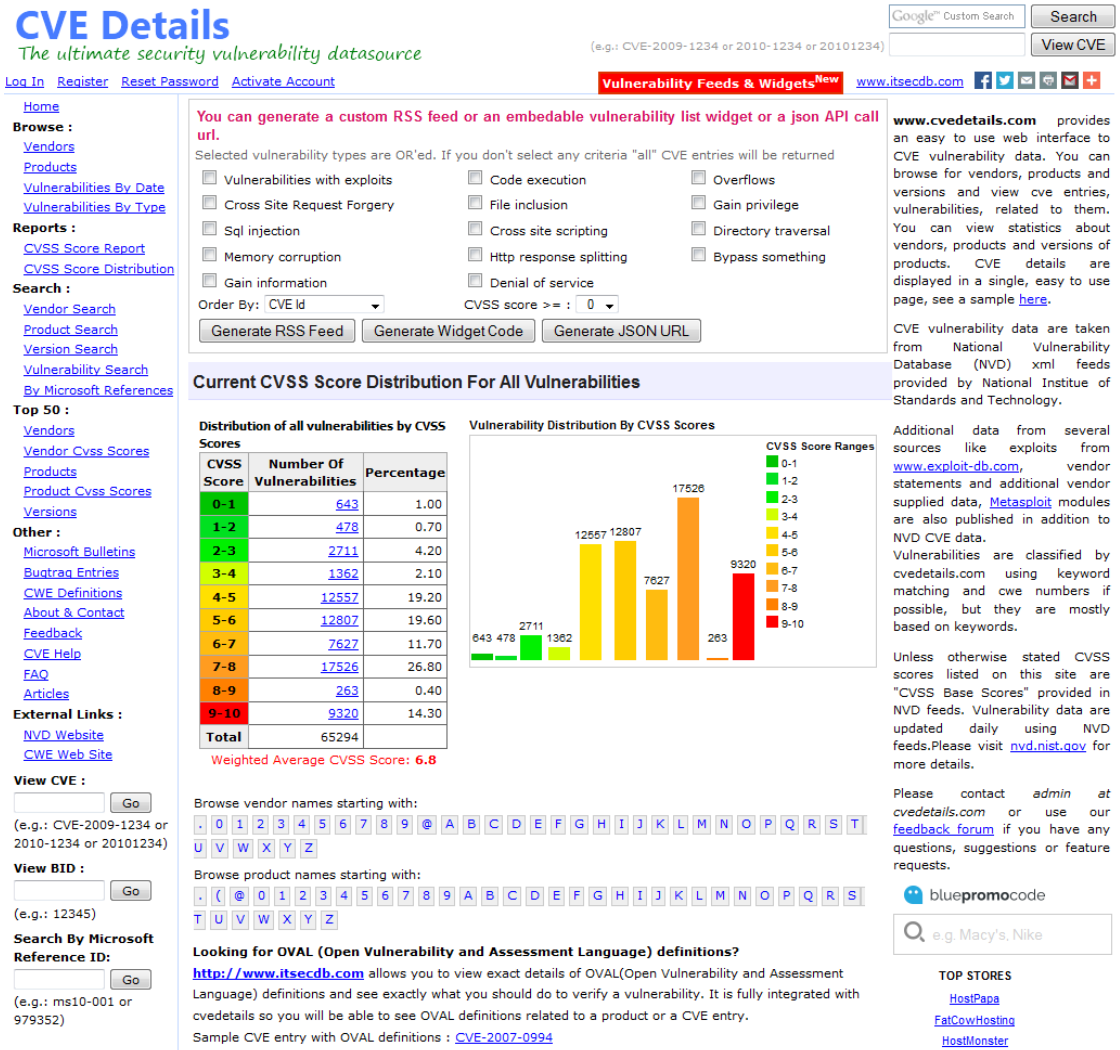
Revisions

- October 17, 2014 Initial Release

Quelle: [US-CERT]

Informationsquellen

CVE-Details



Quelle: [CVE-Details]

Literatur I

[1] ISO/IEC-27002: *Information Technology - Code of Practice for Information Security Management*. Technical Report ISO/IEC 27002:2005(E), ISO/IEO, Juni 2005.

[2] ISO/IEC-Guide73b: *Risk Management - Vocabulary*. Technical Report ISO/IEC GUIDE 73:2009(E/F), ISO/IEO, 2009.

[3] MEHARI: *MEHARI 2010: Fundamental concepts and functional specifications*. Methods, Club de la Securité de l'Information Français, August 2010. http://www.clusif.fr/en/clusif/present/; visited: Oct., 2013.