Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Information Security Management
03 Frameworks – NIST CSFW, IKT Minimalstandard etc.

HSLU – Informatik

Mathias Bücherl (M.Sc.)

Tel. +41 79 746 10 98

mathias.buecherl@hslu.ch

Ziele

- Sie kennen die Struktur und Grundziele des NIST CyberSecurity Frameworks
- Sie können den IKT Minimalstandard zuordnen und anwenden
- Sie haben von weiteren Standards gehört

AGENDA

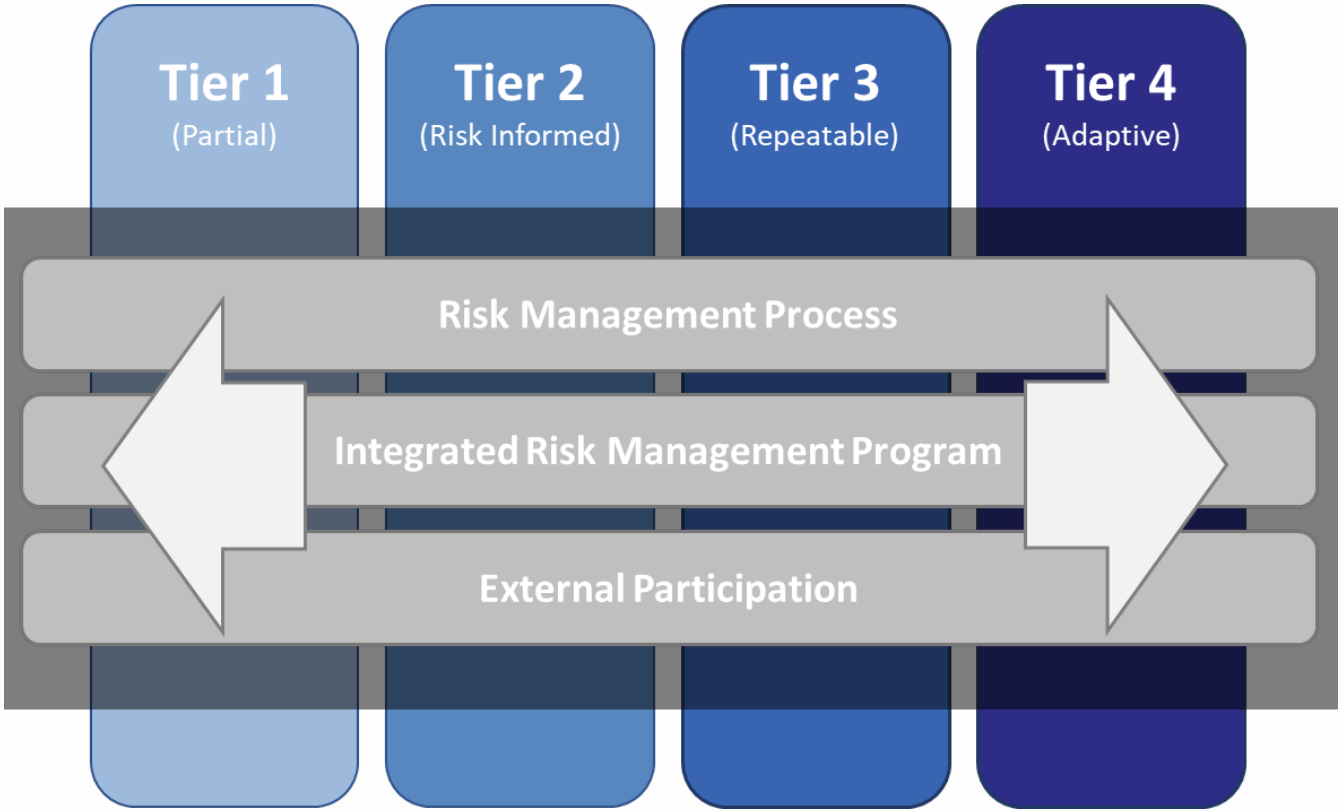
1. **Überblick über das NIST CSFW**
2. Der IKT Minimalstandard
3. Weitere Standards

Cybersecurity Framework Components

Das NIST Framework besteht aus drei Komponenten

https://www.nist.gov/cyberframework

Framework Implementation Tiers



Framework Core

	Function	Category	ID
What processes and assets need protection?	Identify	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
		Supply Chain Risk Management	ID.SC
What safeguards are available?	Protect	Identity Management & Access Control	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes & Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
What techniques can identify incidents?	Detect	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
What techniques can contain impacts of incidents?	Respond	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
What techniques can restore capabilities?	Recover	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

The Five Functions

- Highest level of abstraction in the core
- Represent five key pillars of a successful and wholistic cybersecurity program
- Aid organizations in expressing their management of cybersecurity risk at a high level

The Identify Function

The Identify Function assists in developing an organizational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities

Example Outcomes:

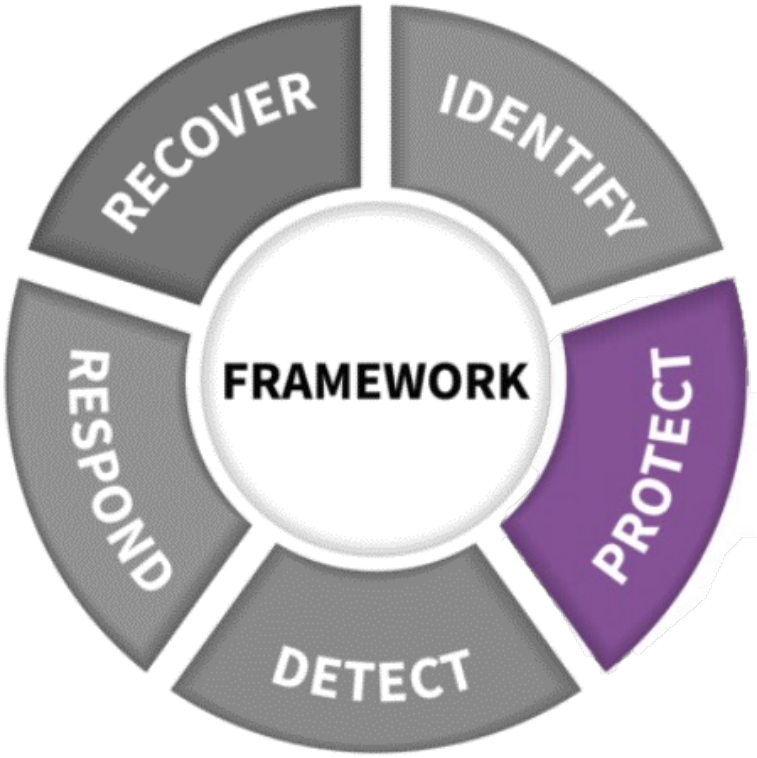
- Identifying physical and software assets to establish an Asset Management program
- Identifying cybersecurity policies to define a Governance program
- Identifying a Risk Management Strategy for the organization

The Protect Function

The Protect Function supports the ability to limit or contain the impact of potential cybersecurity events and outlines safeguards for delivery of critical services

Example Outcomes:

- Data Security protects confidentiality, integrity, and availability
- Protective Technology ensures security and resilience of systems and assists
- Empowering staff within the organization through Awareness and Training



The Detect Function

The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event in a timely manner

Example Outcomes:

- Continuous Monitoring capabilities to monitor cybersecurity events
- Ensuring Anomalies and Events are detected, and their potential impact is understood
- Verifying the effectiveness of protective measures

The Respond Function

The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident to minimize impact

Example Outcomes:

- Ensuring Response Planning processes are executed during and after an incident
- Managing Communications during and after an event
- Analyzing effectiveness of response activities

The Recover Function

The Recover Function identifies appropriate activities to maintain plans for resilience and to restore services impaired during cybersecurity incidents

Example Outcomes:

- Ensuring the organization implements Recovery Planning processes and procedures
- Implementing improvements based on lessons learned
- Coordinating communications during recovery activities

Subcategories & Informative References

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management & Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Cybersecurity Framework Component – ID Example

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9

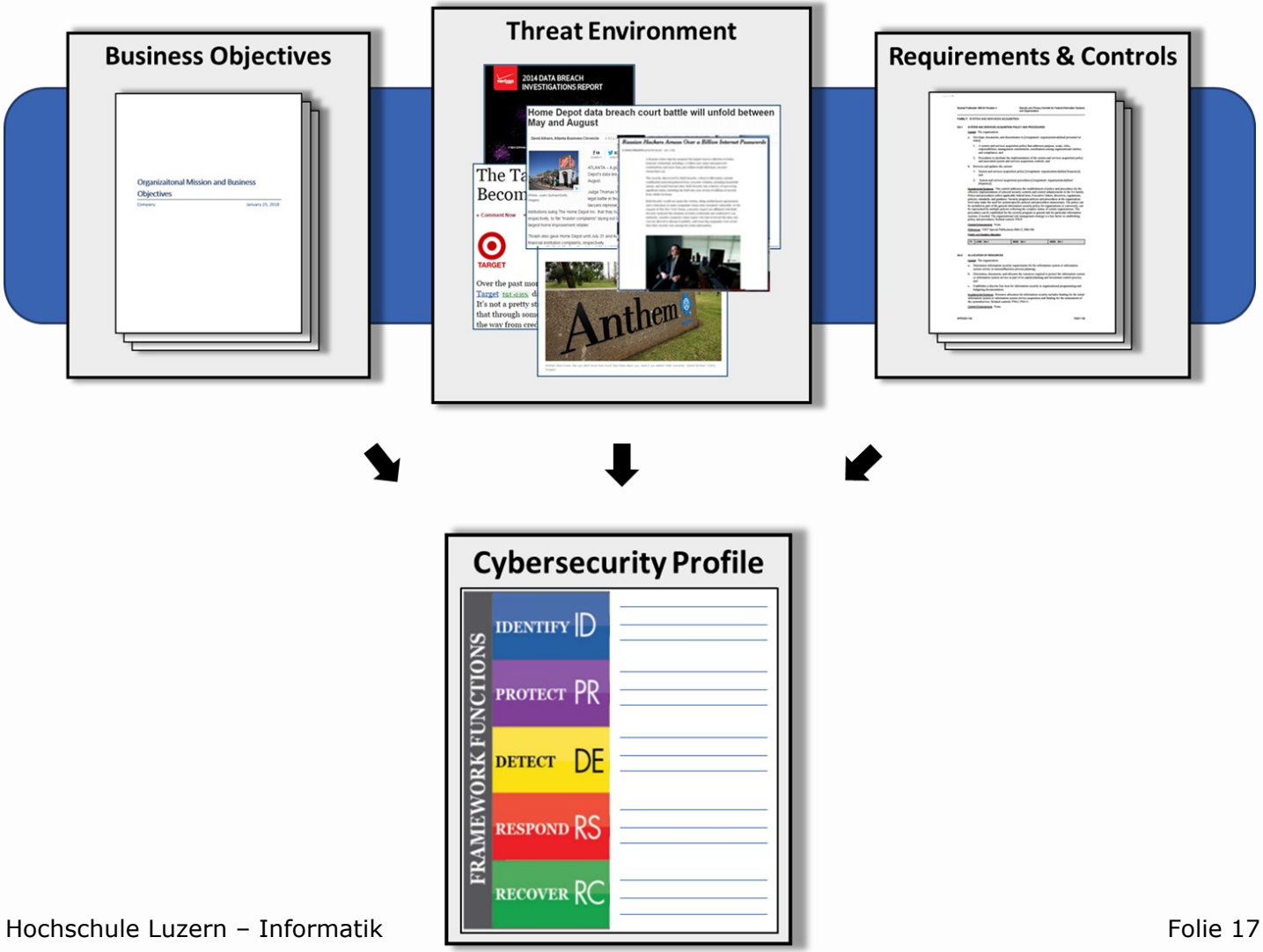
Cybersecurity Framework Component – PR Example

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

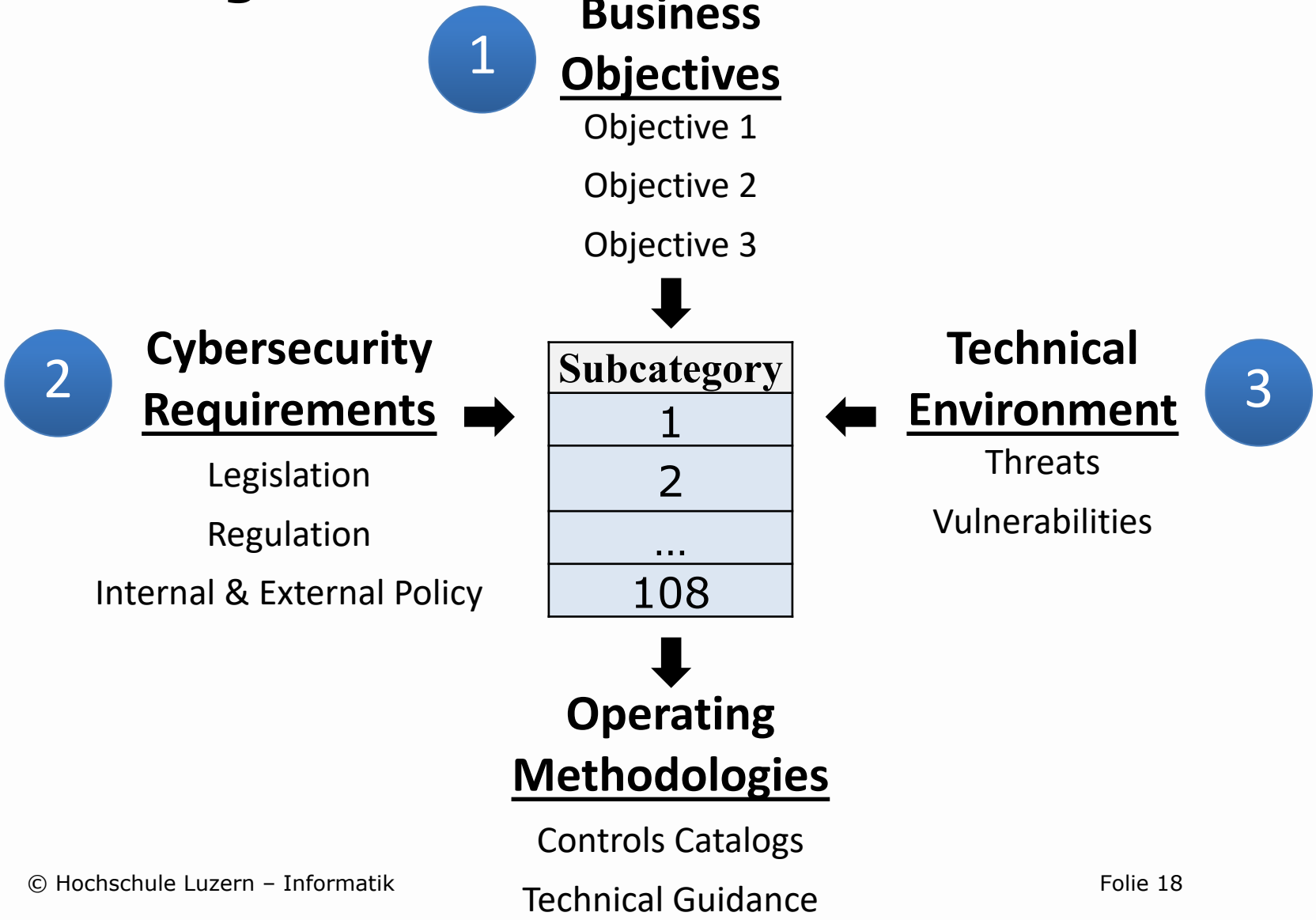
Cybersecurity Framework Component – RS Example

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensics are performed	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15

Building a Profile



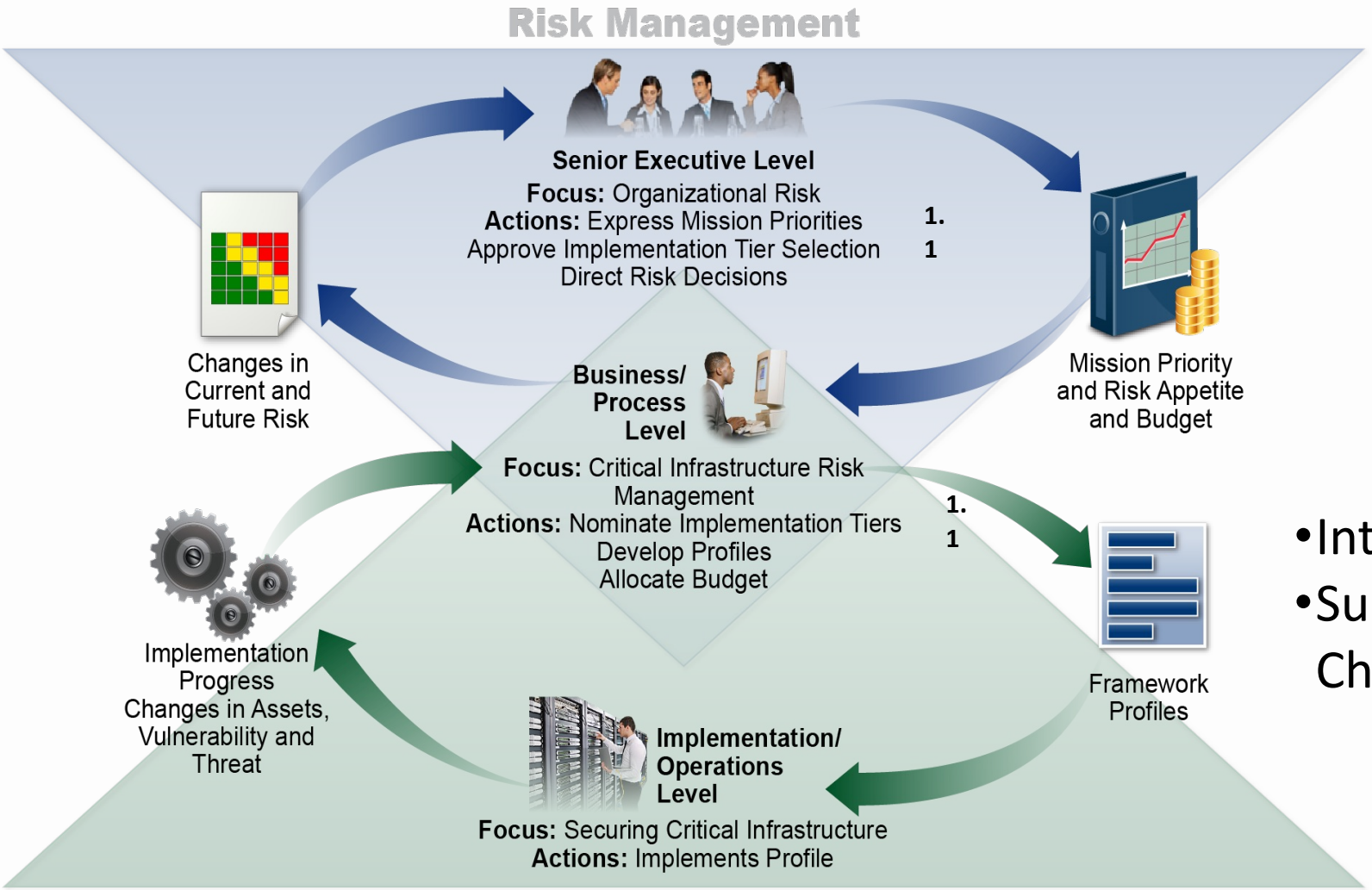
Building a Profile



Seven Step Process

- **Step 1:** Prioritize and Scope
  - Implementation Tiers may be used to express varying risk tolerances[1.1]
- **Step 2:** Orient
- **Step 3:** Create a Current Profile
- **Step 4:** Conduct a Risk Assessment
- **Step 5:** Create a Target Profile
  - When used in conjunction with an Implementation Tier, characteristics of the Tier level should be reflected in the desired cybersecurity outcomes[1.1]
- **Step 6:** Determine, Analyze, and Prioritize Gaps
- **Step 7:** Implementation Action Plan

Supporting Risk Management with Framework



- Internal
- Supply Chain

AGENDA

1. Überblick über das NIST CSFW
2. **Der IKT Minimalstandard**
3. Weitere Standards

Der IKT Minimalstandard

https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html

Aufbau

1. Grundlagen
Dieser Teil dient als Nachschlagewerk und soll Hintergrundinformationen zur IKT-Sicherheit vermitteln.

2. Das **Framework**
bietet den Anwendern, gegliedert nach den fünf Themenbereichen «Identifizieren», «Schützen», «Detektieren», «Reagieren» und «Wiederherstellen», ein Bündel konkreter Massnahmen zur Umsetzung an.

Total handelt es sich um 106 Massnahmen.

3. Mit dem **Self-Assessment** und dem zugehörigen Bewertungstool (Excel) können die Organisationen und Unternehmen den Umsetzungsstand der Massnahmen beurteilen, respektive auch durch externe Firmen prüfen lassen (Audit).

Die Ergebnisse können als Grundlage für ein organisationsübergreifendes Benchmarking verwendet werden.

Grundlagen

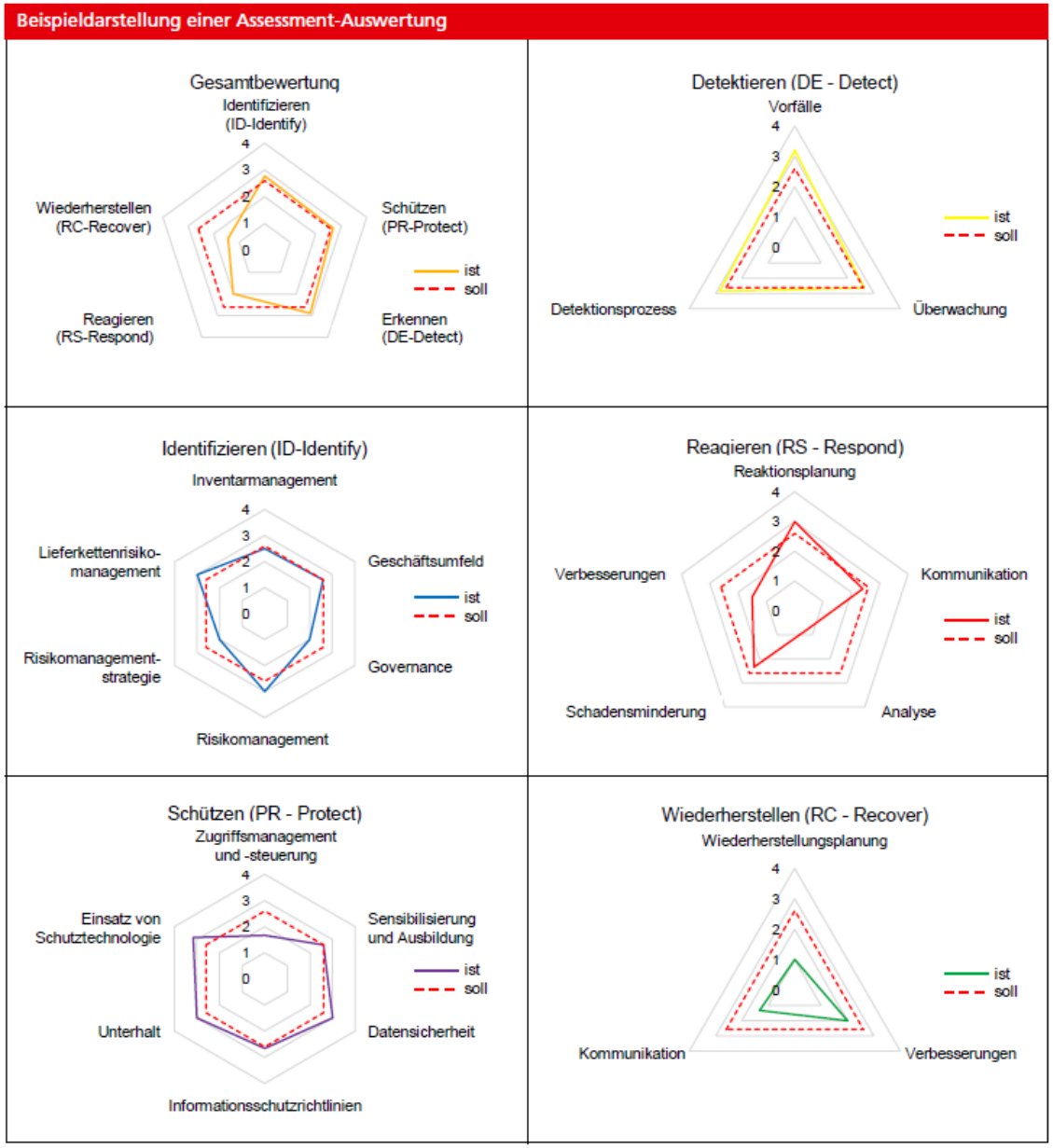
Umsetzung

Prüfung

Defence in Depth

Elemente einer Defense-in-Depth-Strategie	
Risk Management Programm	• Identifizierung von Sicherheitsrisiken • Risikoprofil • Akkurate Bestandsverwaltung der IKT-Betriebsmittel
Cybersecurity-Architektur	• Standards/Empfehlungen • Richtlinien • Vorgehensweise
Physische Sicherheit	• Schutz von Endgeräten • Kontrollzentrum, Zugangskontrollen • Videoüberwachung, Zugangskontrollen & Barrieren
Netzwerk-Architektur	• Typische Sicherheitszonen • Demilitarized Zones (DMZ) • Virtual LANs
Netzwerk Perimeter Security	• Firewalls • Fernzugriff & Authentifizierung • Jump Servers/Hosts
Host Security	• Patch- & Schwachstellen-Management • Endgeräte • Virtuelle Geräte
Security Überwachung	• Intrusion Detection Systems • Sicherheits-Audit-Logging • Sicherheitsvorfall und Event-Überwachung
Vendor Management	• Lieferketten Überwachung & Management • Managed Services & Outsourcing • Nutzung von Cloud-Diensten
Das Element Mensch	• Richtlinien • Vorgehensweisen • Training und Wahrnehmung

Prüfung


Beispieldarstellung einer Assessment-Auswertung
Gesamtbewertung
Identifizieren (ID-Identify)
Schützen (PR-Protect)
Erkennen (DE-Detect)
Reagieren (RS-Respond)
Wiederherstellen (RC-Recover)
ist
soll
Detektieren (DE - Detect)
Vorfälle
Überwachung
Detektionsprozess
Identifizieren (ID-Identify)
Inventarmanagement
Geschäftsumfeld
Governance
Risikomanagement
Risikomanagement-strategie
Lieferkettenrisiko-management
Reagieren (RS - Respond)
Reaktionsplanung
Kommunikation
Analyse
Schadensminderung
Verbesserungen
Schützen (PR - Protect)
Zugriffsmanagement und -steuerung
Sensibilisierung und Ausbildung
Datensicherheit
Informationsschutzrichtlinien
Unterhalt
Einsatz von Schutztechnologie
Wiederherstellen (RC - Recover)
Wiederherstellungsplanung
Verbesserungen
Kommunikation

Gruppenübung – Das Self-Assessment-Tool

- Excel-Datei auf Ilias öffnen und durchsehen
- Wie ist das Self-Assessment-Tool aufgebaut?
- Woher stammt die Struktur?
- Auf welchen Dokumenten basiert es?
- Wie verhält es sich in der Anwendbarkeit für verschiedene Unternehmen / Organisationen?
- Wie unterscheidet sich dessen Zielsetzung für kritische Infrastrukturen / andere Bereiche?

AGENDA

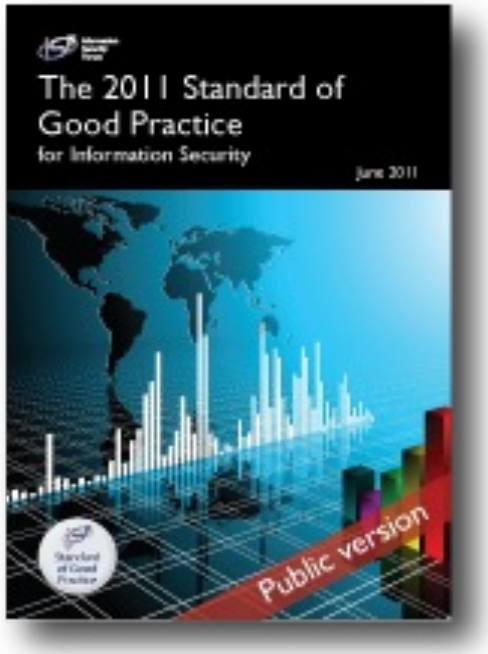
1. Überblick über das NIST CSFW
2. Der IKT Minimalstandard
3. **Weitere Standards und Frameworks**

Weitere Standards

- COBIT (Control Objectives for Information and Related Technology): Framework zur IT-Governance
- ITIL
- Information Security Forum (ISF): Standard of Good Practice for Information Security
- Weisungen über die Informatiksicherheit in der Bundesverwaltung WIsB
- Österreichisches Informationssicherheitshandbuch: https://www.sicherheitshandbuch.gv.at/
- Informationssicherheitshandbuch für die Praxis: www.sihb.ch
- Etc.

Information Security Forum (ISF) - Standard of Good Practice for Information Security

- Businessfokussierter Leitfaden zur Identifikation und zum Management von Informationssicherheitsrisiken in Organisationen
- Basiert auf Erfahrungen von über 260 grossen, weltweit tätigen Organisationen
- Berücksichtigt auch andere Standards (COBIT, PCI DSS, ISO 27001/2, SOX etc.)
- Kann als Grundlage für den Aufbau eines ISMS dienen



Information Security Forum (ISF) - Standard of Good Practice for Information Security

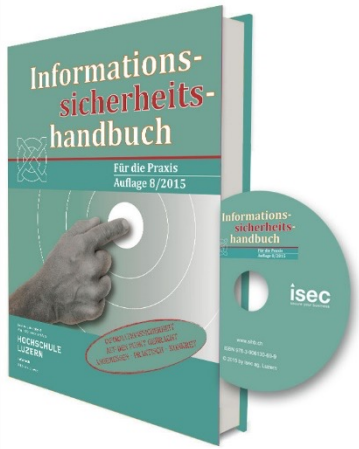
- Wird jährlich aktualisiert
- Unterstützt ein Benchmarking-Programm zur Messung der eigenen Security-Performance gegenüber dem Standard
- Aufgebaut nach 6 Kategorien, auch Aspekte genannt
  - Security Management (enterprise-wide)
  - Critical Business Applications
  - Computer Installations
  - Networks
  - Systems Development
  - End User Environment

Österreichisches Informationssicherheitshandbuch Inhaltsverzeichnis

http://www.sicherheitshandbuch.gv.at/

Informationssicherheitshandbuch für die Praxis

- „Betty Bossi“ für Informationssicherheit
- Praxistipps für den Umgang mit Sicherheit in KMU und KMV
- Analysetool für FirstCut
- Enthält Checklisten und Vorlagen
- Konzentriert sich auf das Wesentliche
  ➔ Mut zur Lücke



http://www.sihb.ch/