RTR

We stand for competition and media diversity

Risk assessment of the Austrian ICT sector

Ulrich Latzenhofer
Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR)

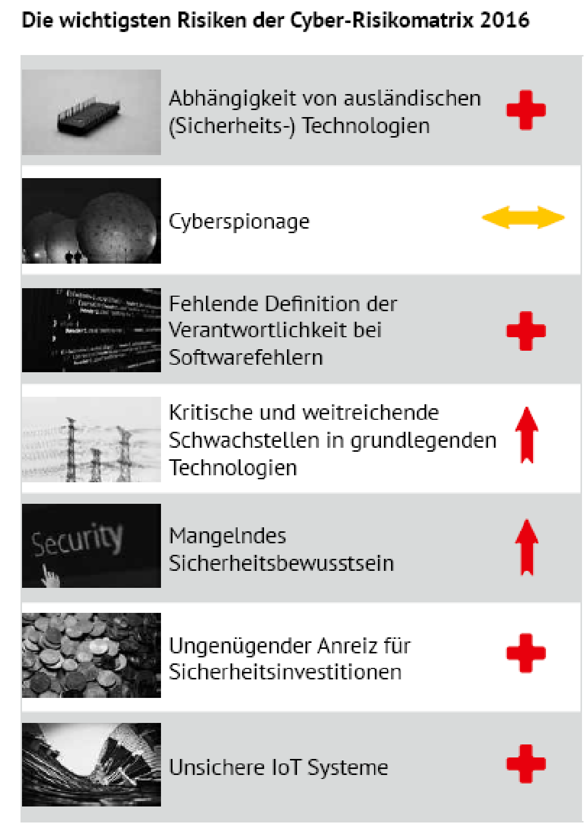
NBU/ENISA workshop on the NIS Directive and Critical Information Infrastructure Protection, 30 Nov. 2018

Agenda

- Background
- Process
- Results and recommendations
- Outlook

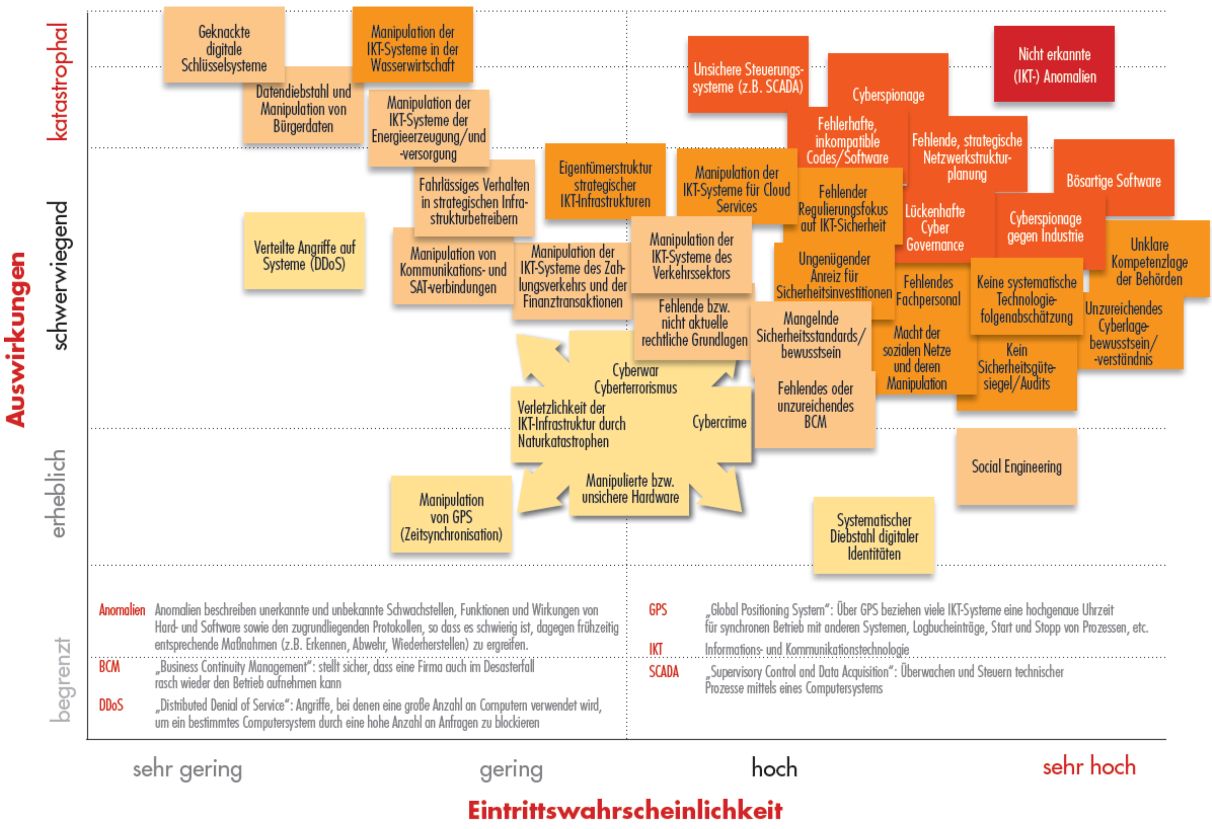
Background

KSÖ cyber risk matrix 2011 (update 2016)



Die wichtigsten Risiken der Cyber-Risikomatrix 2016

	Abhängigkeit von ausländischen (Sicherheits-) Technologien	✚
	Cyberspionage	↔
	Fehlende Definition der Verantwortlichkeit bei Softwarefehlern	✚
	Kritische und weitreichende Schwachstellen in grundlegenden Technologien	↑
	Mangelndes Sicherheitsbewusstsein	↑
	Ungenügender Anreiz für Sicherheitsinvestitionen	✚
	Unsichere IoT Systeme	✚



Auswirkungen

katastrophal

schwerwiegend

erheblich

begrenzt

Geknackte digitale Schlüsselsysteme

Manipulation der IKT-Systeme in der Wasserwirtschaft

Datendiebstahl und Manipulation von Bürgerdaten

Manipulation der IKT-Systeme der Energieerzeugung/und -versorgung

Unsichere Steuerungssysteme (z.B. SCADA)

Cyberspionage

Nicht erkannte (IKT-) Anomalien

Fehlerhafte, inkompatible Codes/Software

Fehlende, strategische Netzwerkstrukturplanung

Bösartige Software

Fahrlässiges Verhalten in strategischen Infrastrukturbetreibern

Eigentümerstruktur strategischer IKT-Infrastrukturen

Manipulation der IKT-Systeme für Cloud Services

Fehlender Regulierungsfokus auf IKT-Sicherheit

Lückenhafte Cyber Governance

Cyberspionage gegen Industrie

Unklare Kompetenzlage der Behörden

Verteilte Angriffe auf Systeme (DDoS)

Manipulation von Kommunikations- und SAT-verbindungen

Manipulation der IKT-Systeme des Zahlungsverkehrs und der Finanztransaktionen

Manipulation der IKT-Systeme des Verkehrssektors

Ungenügender Anreiz für Sicherheitsinvestitionen

Fehlendes Fachpersonal

Keine systematische Technologiefolgenabschätzung

Unzureichendes Cyberlagebewusstsein/-verständnis

Fehlende bzw. nicht aktuelle rechtliche Grundlagen

Mangelnde Sicherheitsstandards/bewusstsein

Macht der sozialen Netze und deren Manipulation

Kein Sicherheitsgütesiegel/Audits

Cyberwar
Cyberterrorismus

Verletzlichkeit der IKT-Infrastruktur durch Naturkatastrophen

Cybercrime

Manipulierte bzw. unsichere Hardware

Fehlendes oder unzureichendes BCM

Social Engineering

Manipulation von GPS (Zeitsynchronisation)

Systematischer Diebstahl digitaler Identitäten

Anomalien Anomalien beschreiben unerkannte und unbekannte Schwachstellen, Funktionen und Wirkungen von Hard- und Software sowie den zugrundliegenden Protokollen, so dass es schwierig ist, dagegen frühzeitig entsprechende Maßnahmen (z.B. Erkennen, Abwehr, Wiederherstellen) zu ergreifen.

BCM „Business Continuity Management“: stellt sicher, dass eine Firma auch im Desasterfall rasch wieder den Betrieb aufnehmen kann

DDoS „Distributed Denial of Service“: Angriffe, bei denen eine große Anzahl an Computern verwendet wird, um ein bestimmtes Computersystem durch eine hohe Anzahl an Anfragen zu blockieren

GPS „Global Positioning System“: Über GPS beziehen viele IKT-Systeme eine hochgenaue Uhrzeit für synchronen Betrieb mit anderen Systemen, Logbucheinträge, Start und Stopp von Prozessen, etc.

IKT Informations- und Kommunikationstechnologie

SCADA „Supervisory Control and Data Acquisition“: Überwachen und Steuern technischer Prozesse mittels eines Computersystems

sehr gering

gering

hoch

sehr hoch

Eintrittswahrscheinlichkeit

Austrian Cyber Security Strategy 2013

Risk analyses for sector-specific cyber threats

- Basis of governmental crisis and continuity management plans
- Part of an integrated cyber security policy: Cooperation with public institutions, economy (in particular operators of critical infrastructures), academia and civil society
- Preparation and regular updates

Risk management

- Comprehensive security architecture (risk and crisis management) for operators of critical infrastructures
- Sector-specific cyber risk management plans also for SMEs, to be coordinated with governmental crisis and continuity management plans
- Measures to increase the level of protection (proportionate to the respective risk)

Austrian Programme for Critical Infrastructure Protection 2014

Risk management for strategic enterprises

- Risk analysis
- Measures for coping with risks

Governmental risk analyses

- Carrying out risk assessment per sector
- Coordination with measures and procedures of national risk analysis
- Alignment with international standards
- Basis for determination of protection standards for strategic enterprises and planning of further measures (situation reports etc.)
- Basis for information and consulting of strategic enterprises by security authorities
- Basis for development of generic measures for reducing identifiable risks

Risk analysis of power industry 2014

REPUCO
UNTERNEHMENSBERATUNG GMBH
bmwfw
E-CONTROL
APG
oesterreichs energie.
BM.I
BUNDESMINISTERIUM FÜR INNERES
bmlvs
INFRAPROTECT GmbH
BUNDESKANZLERAMT ÖSTERREICH

Process

ISO 31000 – risk management

Family of standards related to risk management

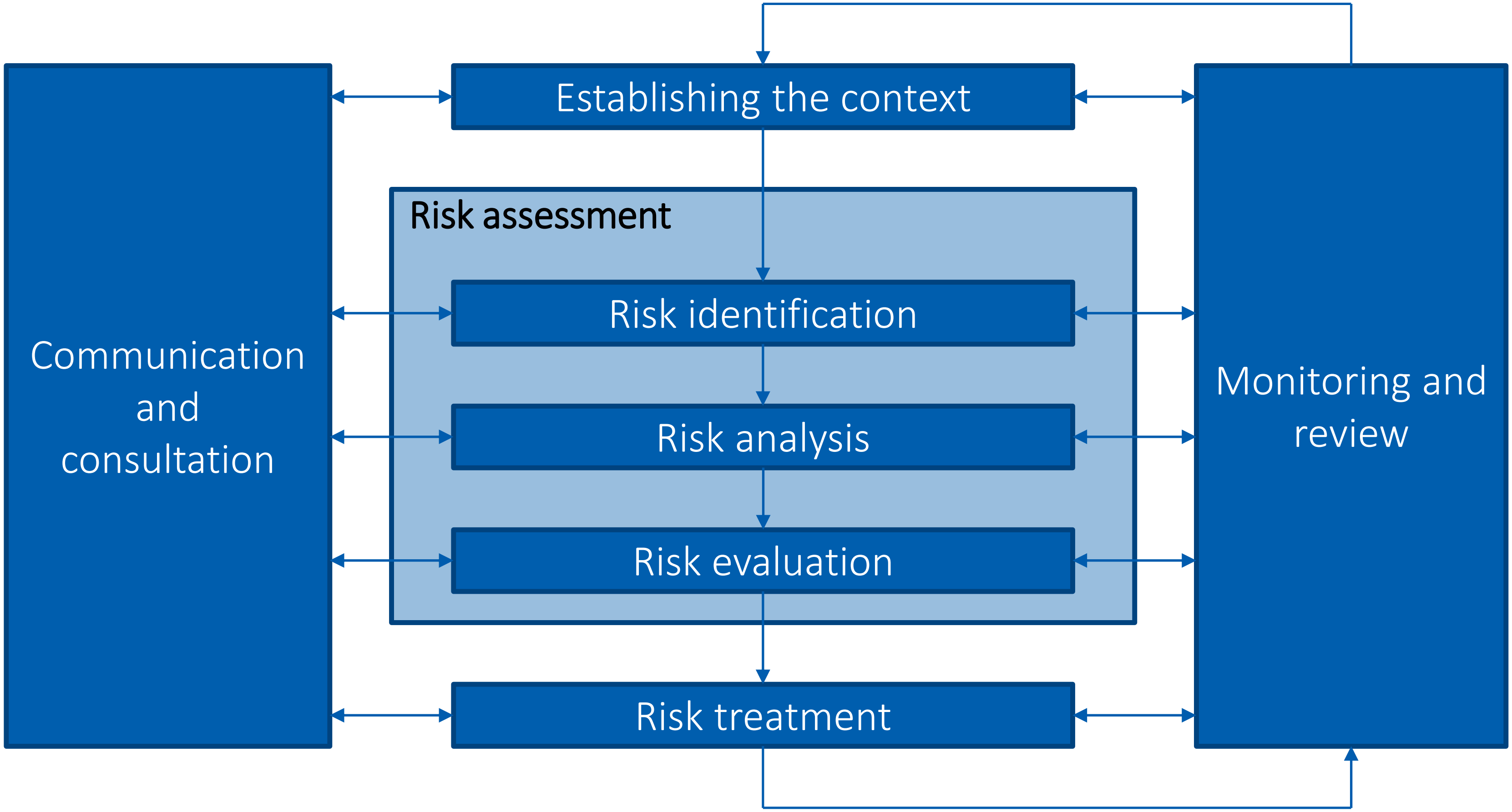
- ISO 31000:2009 – Risk management – Principles and guidelines
- IEC 31010:2009 – Risk management – Risk assessment techniques
- ISO Guide 73:2009 – Risk management – Vocabulary

Management system for design, implementation, maintenance and improvement of risk management processes

Universal but generic approach: for any target audience, for all subjects of risk analyses (in contrast to ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management)

Term *risk:* no longer “chance or probability of loss” but “effect of uncertainty on objectives, activities and requirements”

Risk management based on ISO 31000

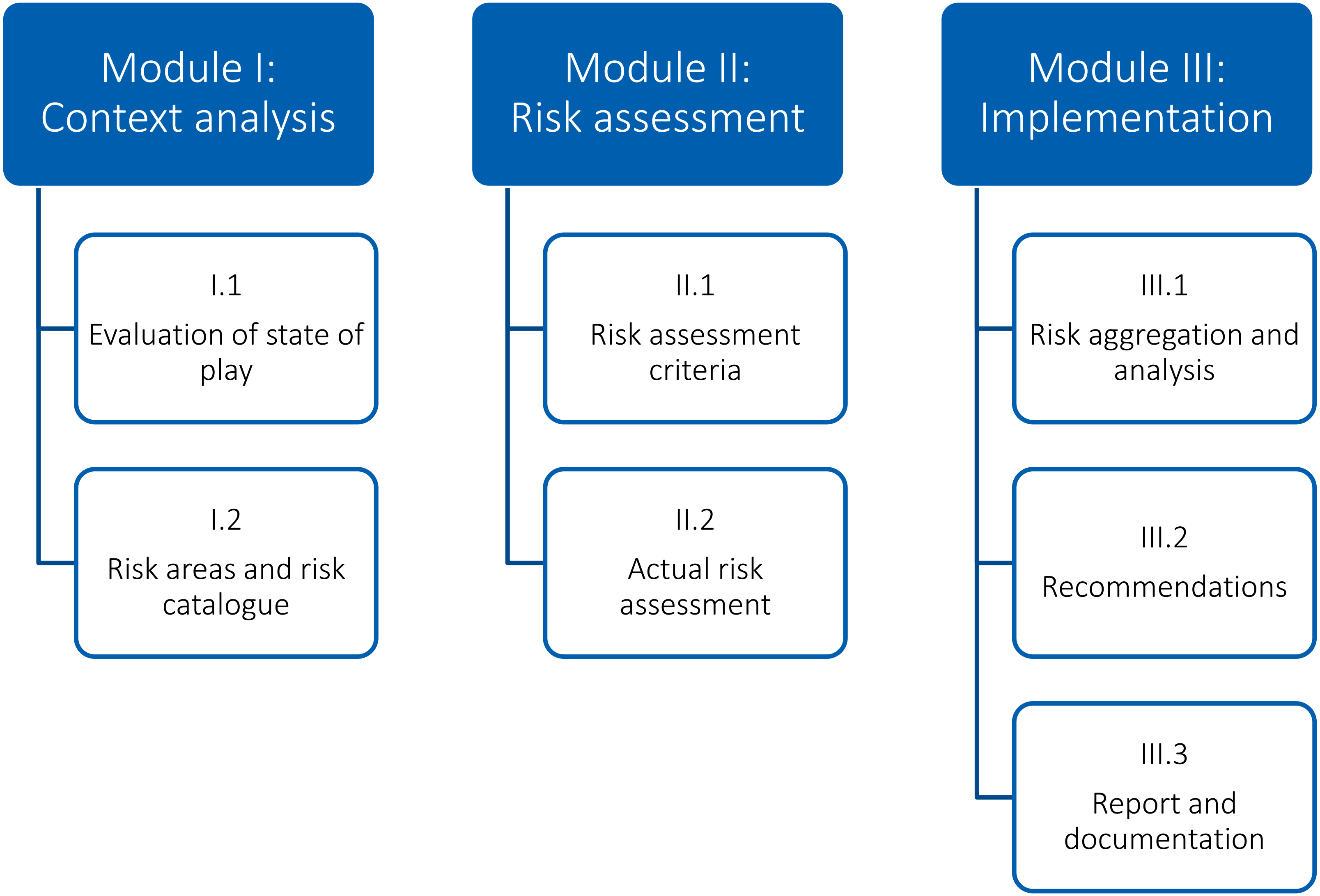


ONR 49000 – Risk management for organisations and systems

Family of ON Rules for implementation of ISO 31000

- ONR 49000 – Terms and basics
- ONR 49001 – Risk management
  (systemic approach, risk management system, risk management process)
- ONR 49002-1 – Guidelines for embedding the risk management in the management system
  (interaction with core processes of the organization, links of risk management with other management subsystems)
- ONR 49002-2 – Guideline for methodologies in risk assessment
  (creativity techniques, scenario analyses in the broader sense, indicator analyses, functional and hazard analysis, statistical analyses)
- ONR 49002-3 – Guidelines for emergency, crisis and business continuity management
  (emergency and crisis scenarios, crisis management team and crisis management process, business continuity management)
- ONR 49003 – Requirements for the qualification of the Risk Manager

Work breakdown structure



Module I:
Context analysis

I.1
Evaluation of state of play

I.2
Risk areas and risk catalogue

Module II:
Risk assessment

II.1
Risk assessment criteria

II.2
Actual risk assessment

Module III:
Implementation

III.1
Risk aggregation and analysis

III.2
Recommendations

III.3
Report and documentation

General principles

Application of proven methods based on standards

- Methods for analysing risk, criticality and vulnerability
- National or international, civil or military standards

Methods of project management

- Structuring into subprojects
- Avoidance or minimisation of project risks

Public-private partnership

- Security not decreed “from above” but lived “from below”
- Voluntary participation of operators and public institutions
- Communication platform for security issues

Project organisation

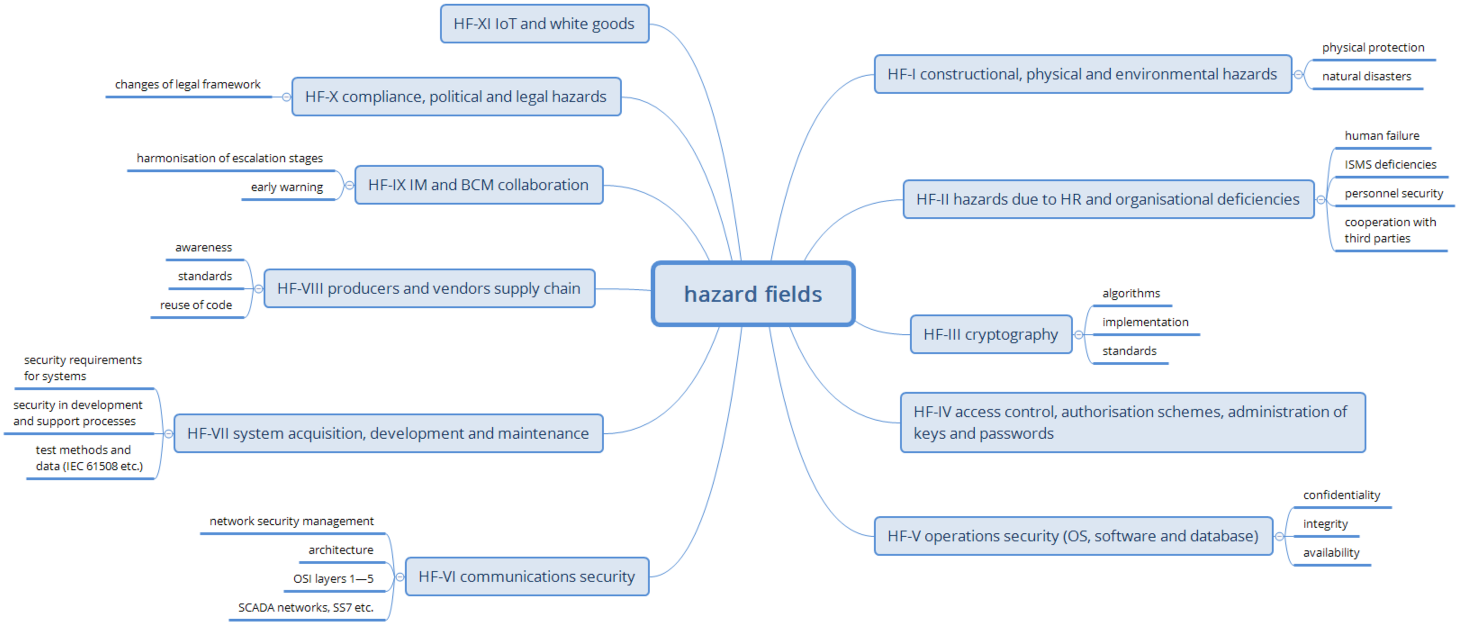
Steering committee

- Interface to Austrian Cyber Security Strategy and Austrian Programme for Critical Infrastructure Protection
- Approval of results
- Four sessions of two hours each

Technical expert group

- Twelve workshops of six hours each (within ten months)
- Additional expert talks

Threats and vulnerabilities (1)



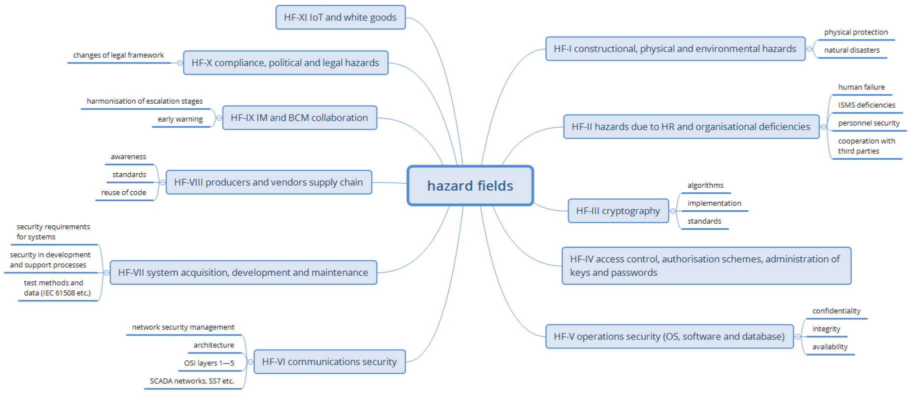
- hazard fields
  - HF-I constructional, physical and environmental hazards
    - physical protection
    - natural disasters
  - HF-II hazards due to HR and organisational deficiencies
    - human failure
    - ISMS deficiencies
    - personnel security
    - cooperation with third parties
  - HF-III cryptography
    - algorithms
    - implementation
    - standards
  - HF-IV access control, authorisation schemes, administration of keys and passwords
  - HF-V operations security (OS, software and database)
    - confidentiality
    - integrity
    - availability
  - HF-VI communications security
    - network security management
    - architecture
    - OSI layers 1—5
    - SCADA networks, SS7 etc.
  - HF-VII system acquisition, development and maintenance
    - security requirements for systems
    - security in development and support processes
    - test methods and data (IEC 61508 etc.)
  - HF-VIII producers and vendors supply chain
    - awareness
    - standards
    - reuse of code
  - HF-IX IM and BCM collaboration
    - harmonisation of escalation stages
    - early warning
  - HF-X compliance, political and legal hazards
    - changes of legal framework
  - HF-XI IoT and white goods

Catalogue of threats and vulnerabilities

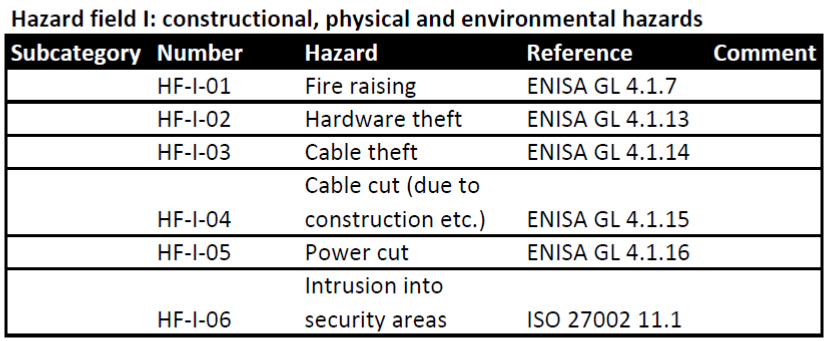
(collected from well-known sources – no need for reinventing the wheel)

- Technical guidelines by ENISA
- Standards and catalogues by BSI, NIST etc.
- National and international standards by ISO, ITU, ETSI etc.
- Completion by involved organisations

Threats and vulnerabilities (2)



- hazard fields
  - HF-I constructional, physical and environmental hazards
    - physical protection
    - natural disasters
  - HF-II hazards due to HR and organisational deficiencies
    - human failure
    - ISMS deficiencies
    - personnel security
    - cooperation with third parties
  - HF-III cryptography
    - algorithms
    - implementation
    - standards
  - HF-IV access control, authorisation schemes, administration of keys and passwords
  - HF-V operations security (OS, software and database)
    - confidentiality
    - integrity
    - availability
  - HF-VI communications security
    - network security management
    - architecture
    - OSI layers 1—5
    - SCADA networks, SS7 etc.
  - HF-VII system acquisition, development and maintenance
    - security requirements for systems
    - security in development and support processes
    - test methods and data (IEC 61508 etc.)
  - HF-VIII producers and vendors supply chain
    - awareness
    - standards
    - reuse of code
  - HF-IX IM and BCM collaboration
    - harmonisation of escalation stages
    - early warning
  - HF-X compliance, political and legal hazards
    - changes of legal framework
  - HF-XI IoT and white goods



Hazard field I: constructional, physical and environmental hazards

Subcategory	Number	Hazard	Reference	Comment
	HF-I-01	Fire raising	ENISA GL 4.1.7	
	HF-I-02	Hardware theft	ENISA GL 4.1.13	
	HF-I-03	Cable theft	ENISA GL 4.1.14	
	HF-I-04	Cable cut (due to construction etc.)	ENISA GL 4.1.15	
	HF-I-05	Power cut	ENISA GL 4.1.16	
	HF-I-06	Intrusion into security areas	ISO 27002 11.1	

I. Physical hazards

II. Organisational deficiencies

III. Cryptography and software

IV. Access control

V. Operations security

VI. Communications security

VII. Life cycle of systems

VIII. Supply chain

IX. Information security and continuity management

X. Compliance

XI. Internet of things, white and brown goods

Criteria of risk assessment

487 threats and vulnerabilities ⇒ 125 individual risks
(technical threats, natural disasters, intentional threats etc.)

Risk = probability (feasibility) x impact

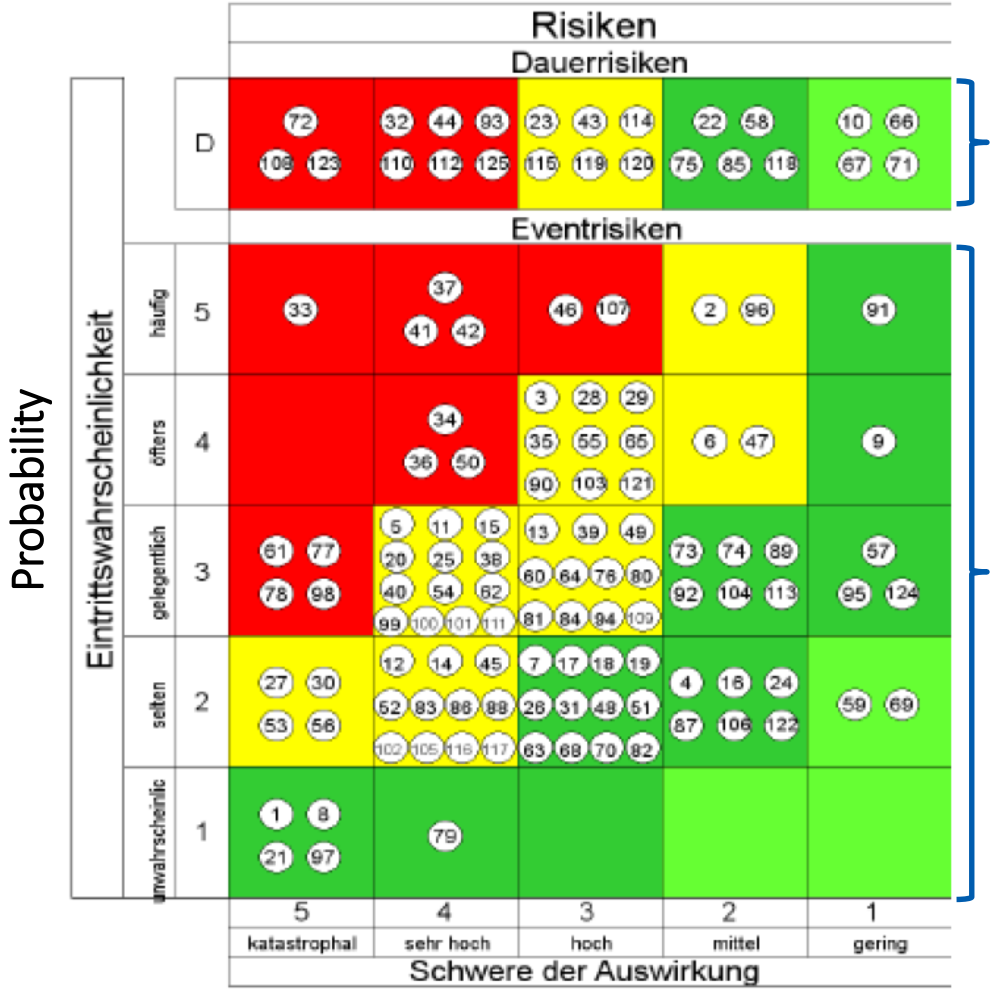
Impact assessment from 1 (low) to 5 (disastrous)

- Quantitative (percentage of annual turnover)
- Qualitative based on security objectives
  - Availability (duration of interruption x number of affected subscribers)
  - Confidentiality
  - Integrity

Assessment of probability (feasibility) from 1 (unlikely) to 5 (frequent)

- Frequency
- Difficulty (complexity, cost) of causing an incident

Individual risks in the worst case



Risiken

Eintrittswahrscheinlichkeit		5 katastrophal	4 sehr hoch	3 hoch	2 mittel	1 gering
Dauerrisiken						
	D	72 108 123	32 44 93 110 112 125	23 43 114 115 119 120	22 58 75 85 118	10 66 67 71
Eventrisiken						
häufig	5	33	37 41 42	46 107	2 96	91
öfters	4		34 36 50	3 28 29 35 55 65 90 103 121	6 47	9
gelegentlich	3	61 77 78 98	5 11 15 20 25 38 40 54 62 99 100 101 111	13 39 49 60 64 76 80 81 84 94 109	73 74 89 92 104 113	57 95 124
selten	2	27 30 53 56	12 14 45 52 83 86 88 102 105 116 117	7 17 18 19 26 31 48 51 63 68 70 82	4 16 24 87 106 122	59 69
unwahrscheinlic	1	1 8 21 97	79			

Schwere der Auswirkung

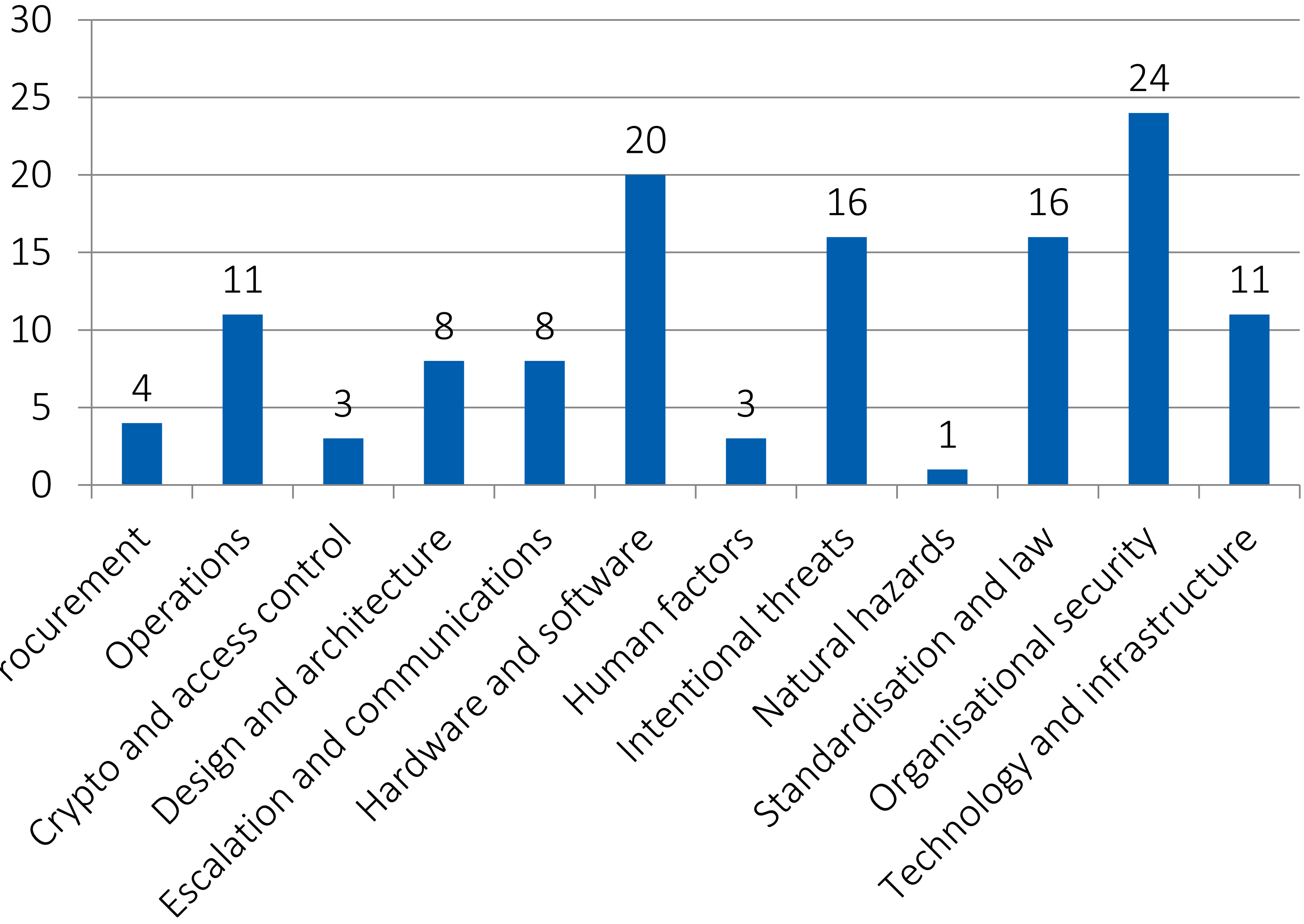
Probability

Permanent risks

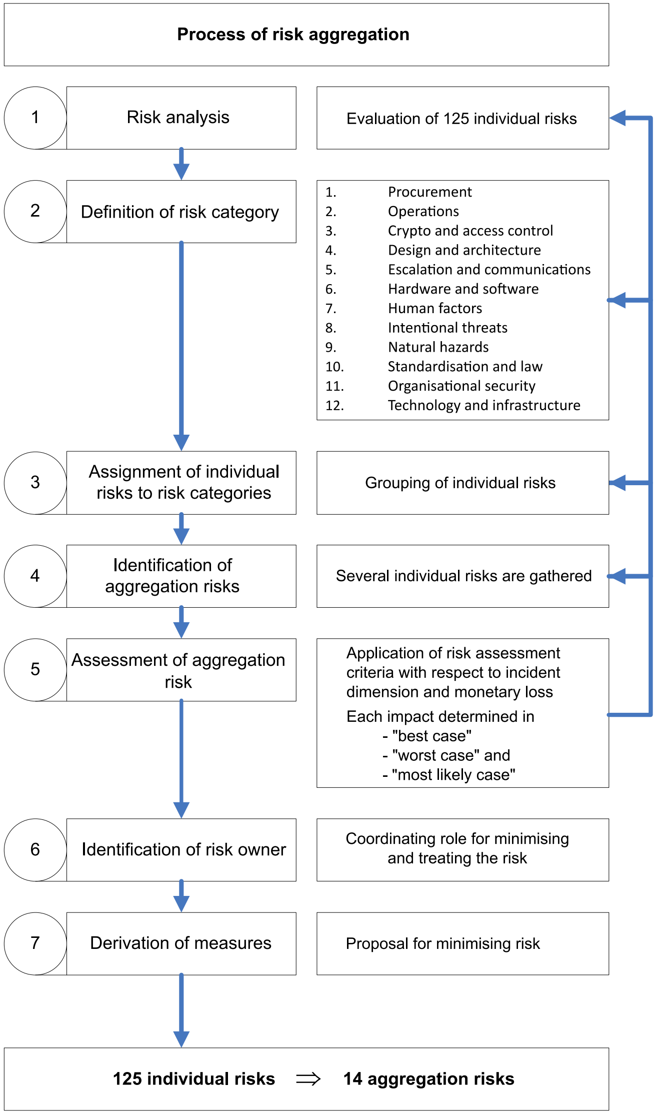
Event risks

Impact

Distribution of individual risks



Risk aggregation



Process of risk aggregation

1 Risk analysis — Evaluation of 125 individual risks

2 Definition of risk category —

1. Procurement
2. Operations
3. Crypto and access control
4. Design and architecture
5. Escalation and communications
6. Hardware and software
7. Human factors
8. Intentional threats
9. Natural hazards
10. Standardisation and law
11. Organisational security
12. Technology and infrastructure

3 Assignment of individual risks to risk categories — Grouping of individual risks

4 Identification of aggregation risks — Several individual risks are gathered

5 Assessment of aggregation risk — Application of risk assessment criteria with respect to incident dimension and monetary loss

Each impact determined in
- "best case"
- "worst case" and
- "most likely case"

6 Identification of risk owner — Coordinating role for minimising and treating the risk

7 Derivation of measures — Proposal for minimising risk

125 individual risks ⇒ 14 aggregation risks

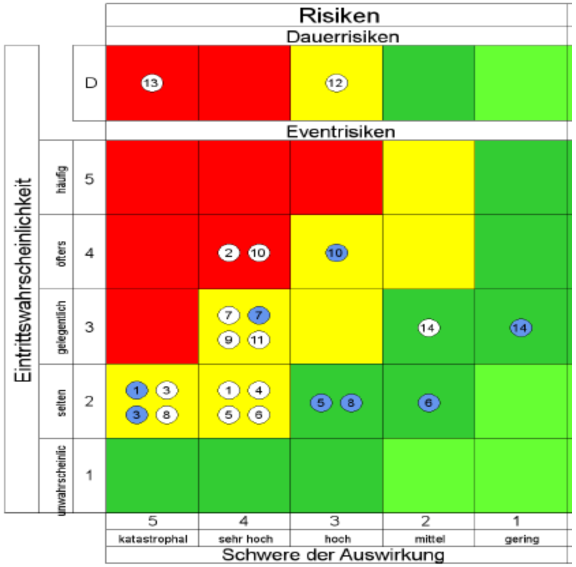
125 individual risks ⇒ 14 aggregation risks

- Failure of essential infrastructures
- Intentional damaging or theft
- Criminal activities from cyber space
- Deficiencies in ICT design and system architecture
- Negative impact of political and legal framework
- Deficiencies in procurement process
- Poor emergency, crisis and business continuity management
- Problems with patch and update process
- Deficiencies in identity and access management (IAM)
- Loss of confidentiality
- Failure of singular ICT suppliers
- Deficiencies in management
- Vulnerabilities in hardware and software
- Lack of compliance

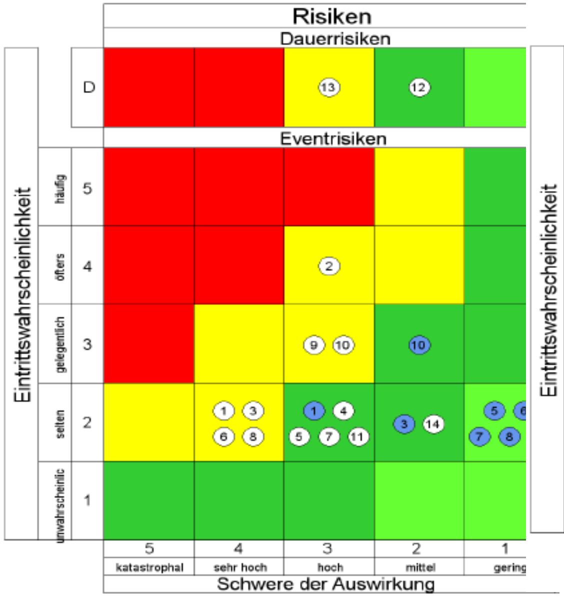
Results and recommendations

Risk matrix for aggregation risks

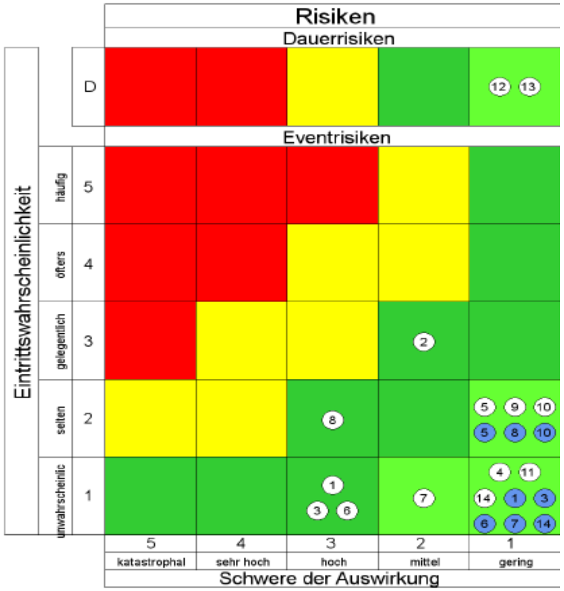
Worst case



Most likely



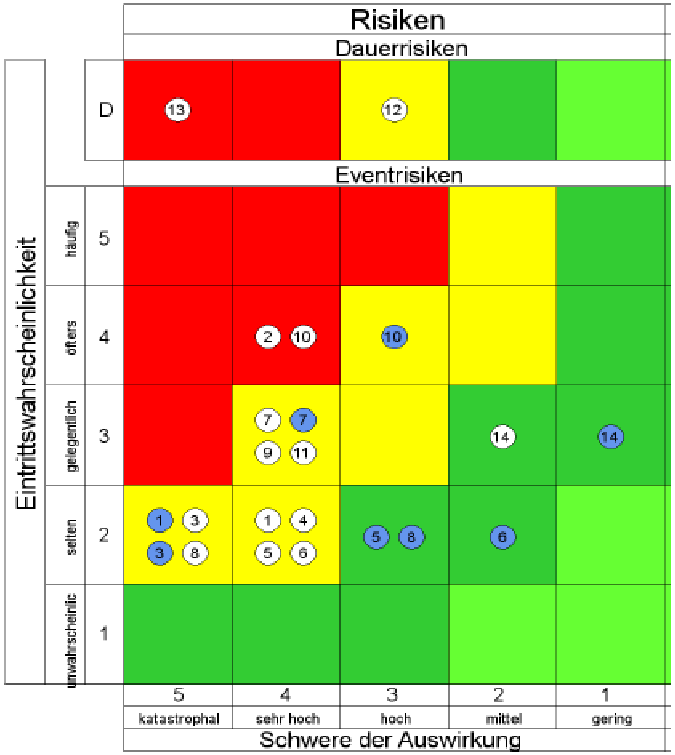
Best case



X-axis: Impact (from “disastrous” to “low”)

Y-axis: Probability (from “unlikely” to “frequent”)

High risks in the “worst case”



13	Vulnerabilities of hardware and software
2	Intentional damaging or theft of important operational resources or equipment
10	Loss of confidentiality of protected information

Medium risks in the “worst case”

7	Deficient emergency, crisis and continuity management
12	Deficiencies in operational management
9	Deficiencies in identity and access management (IAM)
11	Failure or significant service restrictions with singular ICT suppliers
3	Criminal activities from cyber space
8	Significant problems with patch and update process
1	Failure of essential infrastructures
4	Possible significant deficiencies in ICT design and system architecture
5	Negative impact of political and legal framework
6	Deficiencies in procurement process

Recommendations

- 12 risk categories ⇒ 37 recommendations
- 3 groups of process owners
  - Operators of critical infrastructures
  - System-relevant operators
  - Authorities
- Priority from 1 to 3

Recommendations from three perspectives

- Proposals and recommendations directed to organisations
- Suggestions contributing to the definition of a “state of technology” regarding the implementation of information security
- Proposals for future national and international standardisation and legislation which should create a market-neutral framework for implementing information security in the ICT sector

Outlook

Risk management as a permanent process

Ongoing changes

- Technology
- Infrastructure
- Management

⇒ Risk assessment **to be updated regularly** (about every two years)

⇒ Meetings of the technical expert group for **discussing highly topical security issues** even outside the institutional risk assessment process

Extension of the risk assessment’s subject

Risk identification (scoping)

- So far mainly risks affecting the ICT sector
- In the future stronger consideration of interdependencies among different sectors (“cascade effects”)
- Possibly also risks affecting society as a whole

Resources

- Assessment of human and financial resources required for implementing the recommendations

RTR

We stand for competition and media diversity

Thank you for your attention!