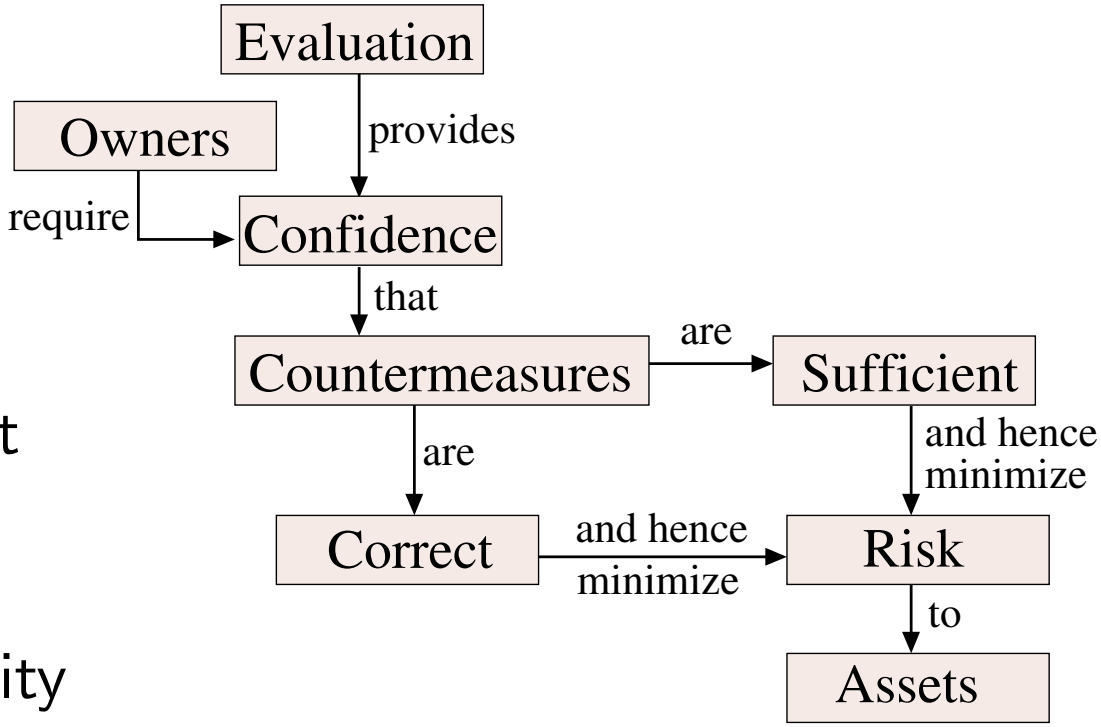
Evaluation Criteria (Standards and Certification)

Security Engineering
David Basin
ETH Zurich

Motivation
Standards



- Testing allows you to check
  if certain requirements are met
- Best practices provide some
  confidence of "baseline" security
- But how do you convince others?

  E.g., your boss, clients, an insurance company, or a jury
- Follow standards and certify this!

Motivation — Assurance

- **Question:** How does the user of a cryptographic device have **confidence** that its output is encrypted using the intended key?

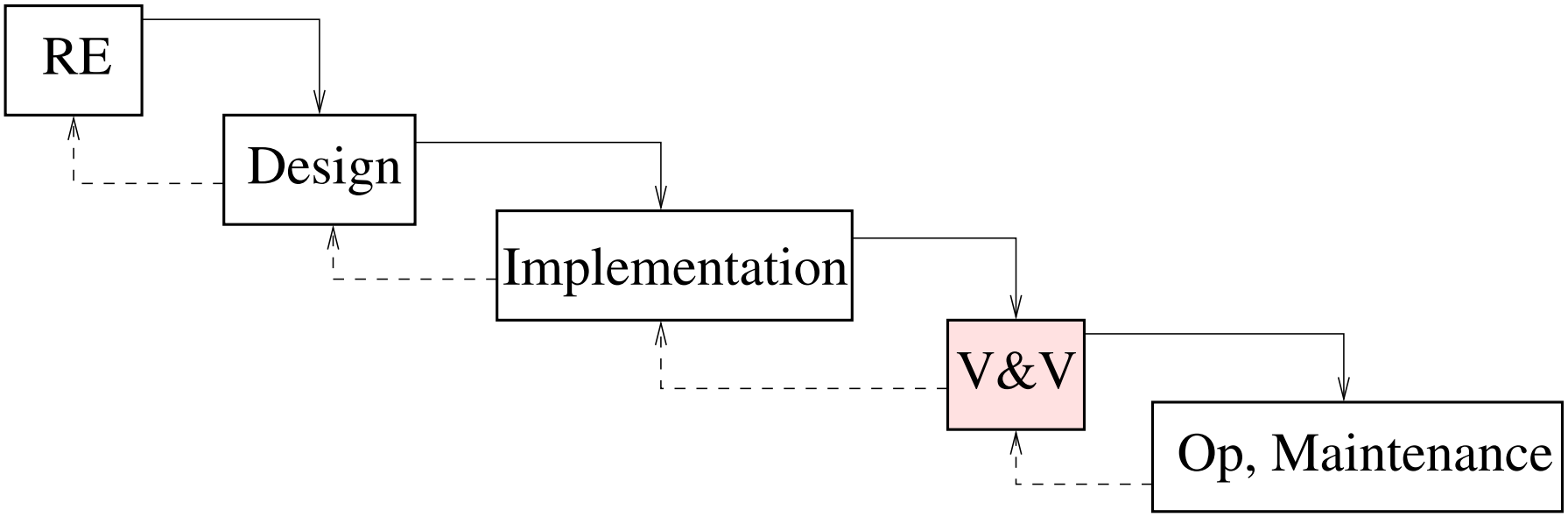
- **Answer:** Crypto provider can supply three kinds of **assurance**:

  1. Evidence that the device was built by well-trained, motivated, and knowledgeable people.
  2. Evidence that the process used to build the device is sound and when properly followed will produce device meeting its spec.
  3. Evidence from testing and analyzing the product directly.

  Which provides strongest evidence?

- US Orange Book pioneered the idea of grouping assurance requirements into increasingly rigorous levels.

Where are we?



Standards cover the entire spectrum.

Evaluation standards usually part of V&V.

Standards and their role

- Standards specify products, services, and processes
- For **products**, standards support interoperability and conformity
  - Originally specified units like distance, weight, and time
  - Critical for physical goods: screws, plugs, train tracks, etc.
  - In computing: instruction sets, protocols, languages, etc.
- Can also be used to provide quantitative and qualitative guarantees about services and **processes**

Example: ISO 9001

- ISO is International Organization for Standardization
- 9001 is a general standard for "quality management systems"
- Requires organizations to have **processes**, e.g. for
  - Identifying customer requirements
  - Formulating quality objectives
  - Controlling purchasing processes
  - Supporting internal communication
- Amounts to a **best practice catalog**
  - Compliance attests that one is giving best effort
  - Certification strengthens this with an "expert" opinion
  - Of course, the **products** can still be lousy!

UNDERWRITERS LABORATORIES INC.

CERTIFICATE OF REGISTRATION

ISO 9000

American NTN Bearing Mfg. Co.

1500 Holmes Road
Elgin, IL 60123

with Remote locations at:

NTN Corporation
Automotive Product
Engineering Department
1578 Higashi-Kaizuka, Iwata-shi
Shizuoka-ken 438 Japan

NTN Bearing Corporation of America
Automotive Center
39255 W. 12 Mile Road
Farmington Hills, MI 48331-2975

NTN Bearing Corporation of America
Central Distribution
76 E. Bradrock
Des Plaines, IL 60018

Underwriters Laboratories Inc.® (UL), Melville, NY, USA, issues this certificate to the Firm named above, after assessing the Firm's quality system and finding it in compliance with

ISO 9001:2000

EN ISO 9001:2000; BS EN ISO 9001:2000; ANSI/ASQ Q9001:2000

for the following scope of registration

3562 (US) : Ball and Roller Bearings
3714 (US) : Motor Vehicle Parts and Accessories

The design and manufacture of angular unit, hub and steel ball bearings for automotive, agricultural and industrial applications.
The remote location at Farmington Hills, MI performs the following primary functions: quality planning, PPAP, contract review, inspection and test, calibration, corrective and preventive action and inventory planning.
The remote location at Des Plaines, IL performs the following primary functions: warehousing, distribution.
The remote location at NTN Corporation, Iwata, Japan performs the following primary functions: Quality Planning and the design of hub and angular unit ball bearings.
Further clarifications regarding the scope of this certificate and the applicability of ISO 9001:2000 requirements may be obtained by consulting the organization.

This quality system registration is included in UL's Directory of Registered Firms and applies to the provision of goods and/or services as specified in the scope of registration from the address(es) shown above. By issuance of this certificate the firm represents that it will maintain its registration in accordance with the applicable requirements. This certificate is not transferable and remains the property of Underwriters Laboratories Inc. ®.

File Number: A5162 Volume: 1of 2
Original Certification Date: June 2, 1997
ISO 9001:2000 Issue Date: May 19, 2003
Revision Date: July 8, 2008
Recertification Date; July 8, 2008
Renewal Date: July 7, 2011

John H. Schmidt
Senior Vice President, Chief Development Officer

ANAB ACCREDITED

UL REGISTERED FIRM

Examples of business standards with impact on IT

- EU directives
  - Protection of personal data (95/46)
  - Privacy and electronic communications (2002/58)
  - Electronic signature (99/93)
  - Money laundering (91/308)
  - Electronic commerce (2000/31)
  - Auditing (78/660, 83/349, 84/253, 2001/256)
- Basel committee
  - Risk management principles for electronic banking (July 2003)
  - Basel II (June 2004)
  - Outsourcing in financial services (Aug 2004)
- Sarbanes-Oxley, Gramm-Leach-Bliley Act, HIPAA, ...

Legal problems and image damage from noncompliance!

Security standards and guidelines

- Objective: gain confidence in a system's security
  - indirectly by evaluating processes or
  - directly by evaluating product
- Many different standards and associated approaches
  - Process recommendations: e.g. train employees in security
  - Product recommendations: e.g. configuring standard products
  - Rarely criteria for evaluating specialized products.
    Common criteria is an exception here.
- Range from best practice catalogs to detailed evaluation standards

Security standards and guidelines (examples)

NIST: National Institute of Standards and Technology

Computer Security Resource Center provides guidelines and principles for building secure systems

ISO/IEC 27000 Series: Information Security Management Systems

Code of practice for ISMS. High-level, mostly nontechnical account of relevant Information Security areas in an organization

Common Criteria (ISO 15408): Criteria for certifying that technical IT systems meet given security requirements

BSI IT Baseline Protection: Comprehensive reference to develop and evaluate Information Security processes and systems

Road map

- Motivation

☞ **NIST**

- ISO/IEC 27000 series
- Common Criteria
- BSI baseline protection (Grundschutz)
- Conclusions

NIST

Publishes **special papers**, ranging from general to specific. E.g.,

SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems

Check list of issues to consider when securing IT Systems

SP 800-123 Guide to General Server Security

SP 800-43 System Administrative Guidance for Windows 2000 Professionals

Useful for hardening in Windows Environment

NIST example: SP 800-14

Contains **8 principles** and **14 practices**, where practices are derived from (possibly multiple) principles. Examples:

Principle: Computer security should be cost-effective

> "The costs and benefits of security should be carefully examined in both monetary and non-monetary terms to ensure that the cost of controls does not exceed expected benefits. Security should be appropriate and proportionate to the value of and the degree of reliance on the IT systems and to the severity, probability, and extent of potential harm. ..."

Practice: Risk management

> "Risk management requires the analysis of risk, relative to potential benefits, consideration of alternatives, and, finally, implementation of what management determines to be the best course of action ..."

NIST example (cont.)

- NIST principles and practices are process oriented

  Nontechnical and neither technology nor product-specific

- More a collection of common-sense best-practices. E.g.,

  "Employees should be trained in the computer security responsibilities and duties associated with their jobs"

  "Any organization should require users to identify themselves uniquely before being allowed to perform any actions on the system unless user anonymity or other factors dictate otherwise."

- Still a useful starting point for developing processes and practices within an organization

NIST example: SP 800-123

Guide to General Server Security (July 2008) is a bit more specific:

4.2 Hardening and Securely Configuring the OS

Administrators should harden and securely configure server OS:
- Remove unnecessary services, applications, and protocols
- Configure OS user authentication, ...

4.2.1 Remove or Disable Unnecessary Services, Applications, and Network Protocols

A server should be on a dedicated, single-purpose host, if possible. When configuring the OS, remove or disable all services and protocols that are not required, e.g.,
- File and printer sharing services (e.g., Windows NetBIOS, file and printer sharing, NFS, FTP)
- Wireless networking services
- Directory services (e.g., LDAP, NIS), ...

Road map

- Motivation
- NIST
- ☞ **ISO/IEC 27000 series**
- Common Criteria
- BSI baseline protection (Grundschutz)
- Conclusions

ISO/IEC 27000 Series

- Standards for Information Security Management Systems
- Risk management approach, aiming at continual improvement

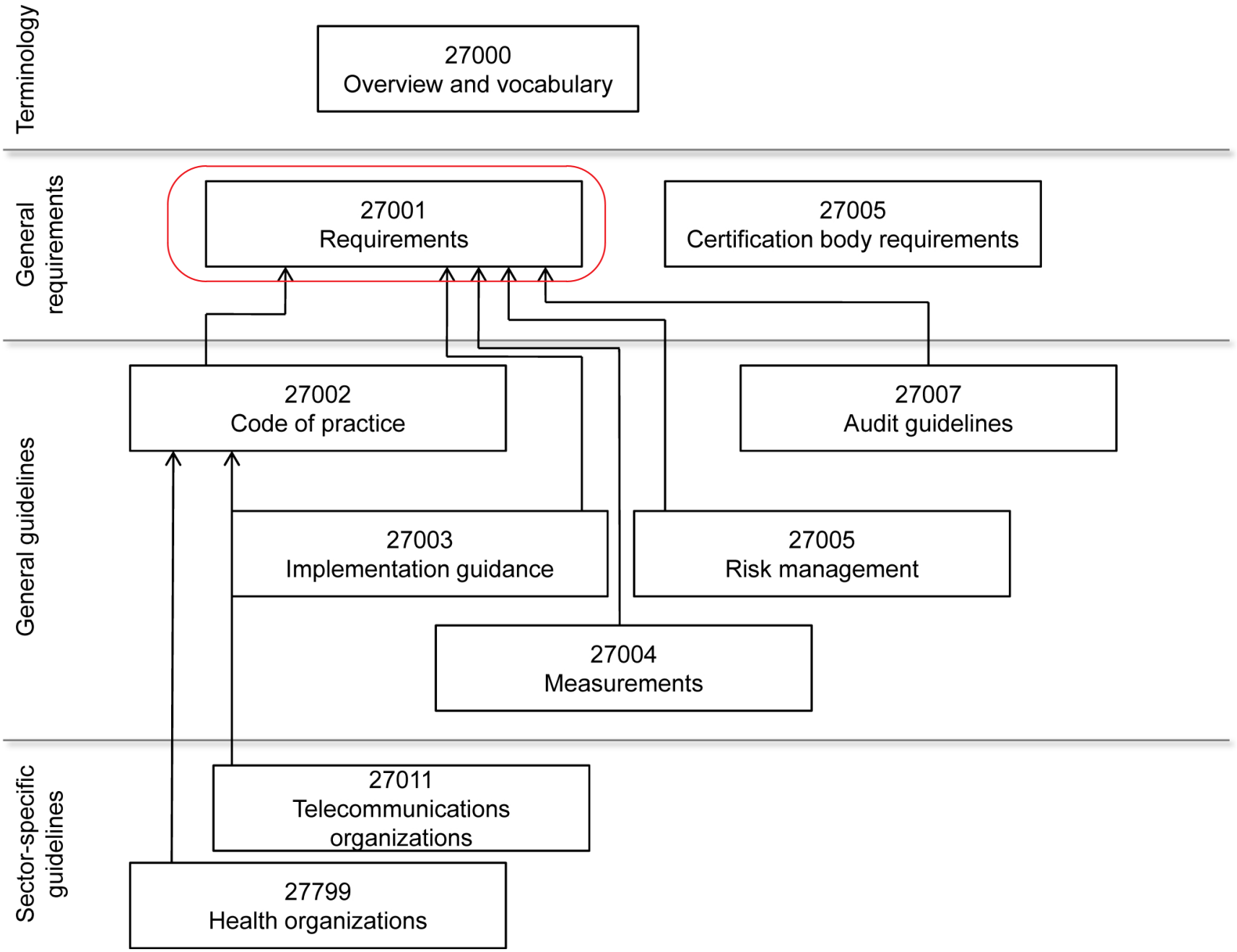
  "Security is a process" not a state, product, etc.
- Evolved from British Standard BS7799 and ISO 17799
- General guidelines
  - Describes areas relevant for initiating, implementing, and maintaining Information Security in organizations
  - High-level, **management-oriented** (neither deep nor technical)
  - Does not provide detailed conformance specifications needed for an in-depth security review
- Certification is possible by (certified) auditors

Management-oriented security guidelines?

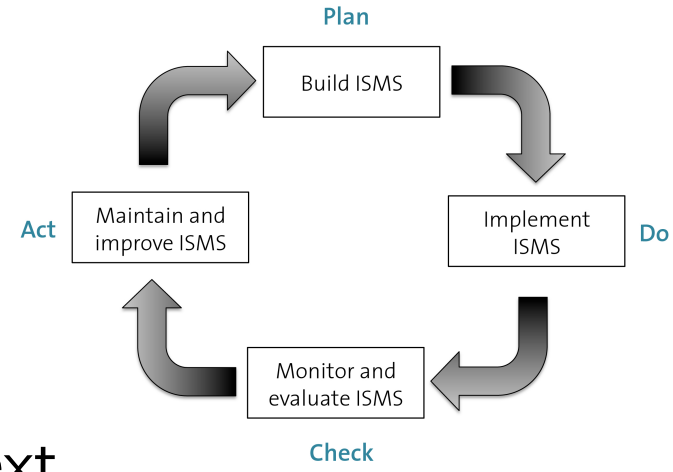
- But isn't security primarily for technologists?
- No, it is also a **management imperative**!
  - **Corporate governance** requires systems for directing and controlling businesses
  - **IT governance** concerns leadership, organizational structures, business processes, standards and their compliance to ensure IT systems fulfill business objectives
- Various standards require monitoring and controlling IT risk

  E.g., Sarbanes-Oxley, required of all SEC-registered companies
- And without top management commitment and support, security controls often ad-hoc and mismatched with corporate objectives

27000 ISMS standards family



27001 Certification requirements



- ISMS process organized as follows (27001:2005):[1]

  Plan: fix ISMS scope and management context as well as security policy and risk analysis method.

  Do: perform risk assessment and implement improvements.

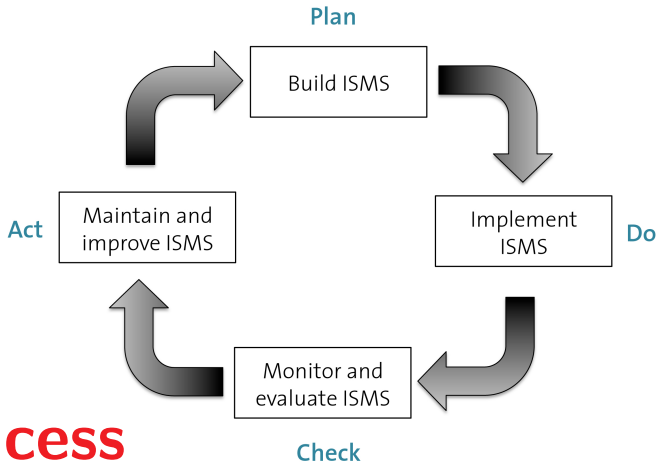
  Check: evaluate performance by measuring results and comparing against objectives. This is where **audits** take place.

  Act: correct and **improve** the ISMS. Learn from mistakes.

- Process structure goes back to Deming, 1950s
  - Variants used in many security audit methodologies
  - **Example BSI Grundschutz**: create security concept, implement it, maintain and improve (includes check, i.e. audits)

[1] 27001:2013 renames phases, increasing emphasis on leadership structure within organization.

27001 (cont.)



- **Risk management** to achieve an effective ISMS through a **continual improvement process**
- Focus on **management processes**.
  - Controls not specified, but ISO/IEC 27002 recommended.
  - Alternative: BSI IT-Grundschutz Methodology
- Certification assumes that if processes are effective, then so are controls, e.g., firewalls are in place and are properly managed.
- This fundamental distinction between **processes** and **products** underlies almost all certification standards.

  In practice, there is considerable confusion on this point

ISO/IEC 27001 certification — audit process

1. **Preliminary, informal review of the ISMS.**

   E.g., check status of organization's information security policy and risk management plan.

2. **Detailed compliance audit against standard.**

   Auditors judge whether ISMS is properly designed and implemented, and if it is in operation. E.g., does a management body regularly meet and oversee ISMS operation?

   Successful audit $\leadsto$ certification
   Unsuccessful audit $\leadsto$ list of problems + corrective actions

3. **Follow-up reviews or audits to confirm that the organization remains in compliance with the standard.**

ISO 27002 — topics addressed (examples)

- Establishing organizational **security policy**
- Organizational **security infrastructure** (management framework)
- **Asset classification and control**. Know what you have (physical, software) and its security classification
- **Personnel security** (e.g., personal screening, training, ...)
- **Physical and environment security** (building, power, ...)
- **Communications and operations management** to ensure correct and secure operation of information processing facilities (network, mail, office systems, ...)
- **Access control** (user registration, privilege management, ...)
- **System development and maintenance** (to ensure that security is built into information systems)

Example from "Access Control"

Change control: Implementation of system changes must be controlled by a formal change-control procedure.

- Proposals for changes should be submitted through a centralized scheme and there should be an audit trail of change requests, decisions made, and rational.
- Existing controls and procedures should be regularly reviewed to ensure they are not compromised by proposed changes.
- All software, hardware, and information assets that may need to be amended by the change must be identified.
- Code changes to sensitive applications should be checked by a second person.
- Version control is required for updates, ...

Example from "Information systems acquisition, development and maintenance"

Input data validation

Data input to application systems should be validated to ensure that it is correct and appropriate. Checks should be applied to the input of business transactions, standing data (names, credit limits) and parameter tables (sales prices, currency conversion rates). The following controls should be considered:

1. Input checks to detect the following errors:
   (a) out-of-range values;
   (b) invalid characters in data fields;
   (c) missing or incomplete data;
   (d) exceeding upper and lower data volume limits;
   (e) unauthorized or inconsistent control data;
2. Periodic review of the content of key fields or data fields to confirm their validity and integrity. ...

Road map

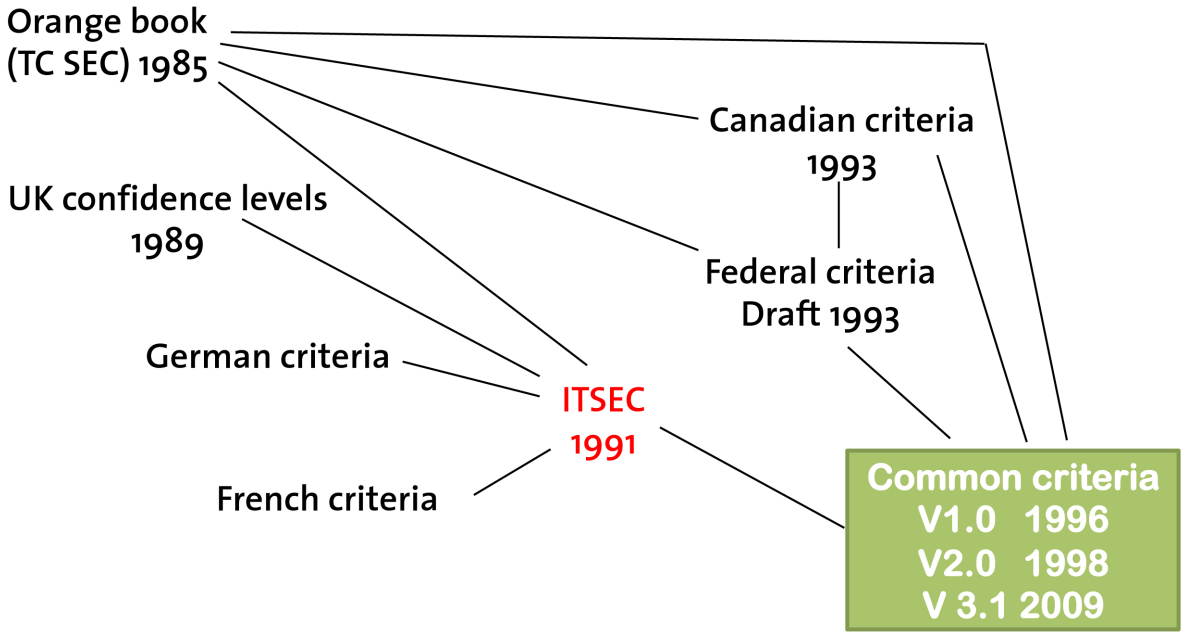
- Motivation
- NIST
- ISO/IEC 27000 series

☞ **Common Criteria**

- BSI baseline protection (Grundschutz)
- Conclusions

Common Criteria

- Evolution of efforts to develop criteria for **developing** and **evaluating products or systems** with security functionality



- Detailed **evaluation methodology**
  - Which security objectives are relevant?
  - Are measures taken adequate to achieve the objectives?
  - Do they work correctly? Deployed and operated correctly? ...

Objective

- Evaluate security properties of IT products and systems
  - Enhance confidence in security by specifying actions to be taken during development, evaluation, and operation
  - Ensure comparable evaluation results across different products
- **Target of Evaluation**
  - OS, computer networks, distributed systems, cryptographic co-processor, application + OS, ...
- Evaluate ToE with respect to standardized **Security Functional Requirements** and **Security Assurance Requirements**
- Successful evaluation results in a certificate

Structure

Part 1. Introduction and general model

- Concepts and principles of IT security evaluation
- General evaluation model
- Constructs for defining IT security requirements

Part 2. Security functional requirements

- Standard way of expressing security requirements
- Catalog of such requirements

Part 3. Security assurance requirements

- Correctness of implementation and effectiveness of security functions
  "Grounds for confidence that an entity meets its security objectives"
- **Evaluation Assurance Levels** describing assurance requirements

Part 1: General model — protection profile

- Specifies security objectives
  - Generally for a class of products.
  - E.g., smart cards used to create digital signatures
- Created by group of users: consumer group, organizations
  - Idea: where possible, re-use earlier experiences
  - Helps vendors: PPs instantiated to **Security Target**
  - Helps consumers: determining product-relevant requirements.
- Must be checked for completeness and lack of contradictions.
  i.e., are themselves evaluated (not said how this is done)
- Implementation independent

Example: PP requirements
Cryptographic key management (sample)

- **Key generation** requires keys to be generated in accordance with a specified algorithm and key sizes.
- **Key distribution** requires keys to be distributed in accordance with a specified distribution method.
- (Similar requirements for **key access** and **destruction**)
- The following actions are possible **management functions**: changes to key attributes including user, key type, validity period, and use (signature, key encryption, data encryption, ...).
- The following actions should be **auditable** if auditing is specified: success and failure of the activity, ...

Example: automatic cash dispensers[2]

OT.INT_DA The ACD/ATM shall enable the AAC (ACD/ATM Controller) to verify the integrity of the authorization request.

OT.INT_RDA Any modification (e.g., response code and authorization number) of the response to the authorization request shall be detectable. The ACD/ATM shall ensure that the response corresponds to the withdrawal in progress.

OT.PIN The PIN shall remain confidential. In particular, it shall not be possible to intercept it unenciphered between the device at which it is entered and the place where it is checked (microcircuit or AAC or issuer).

OT. LECTCLES It shall be impossible for any party to read the cryptographic keys.

OT.LOGICIELS It shall be impossible for unauthorized software to be installed on the ACD/ATM (authorized software is defined in the ST).

OT.MAINT Maintenance (and running) operations must be traced.

---

[2] **Source:** Automatic Cash Dispensers/Teller Machines, Protection Profile v1.0, registered at the French Certification Body, number PP/9907.

Example: (cont.)

OE.INT_CLES Any modification of the cryptographic keys in transit over a network shall be detectable.

OE.CHIF_CLES Any cryptographic key transferred over the telecommunication network shall be encrypted by a key transport key.

OE.INT_AUTO Any modification of the card identification elements, of the authorization amount, of the number of the ACD/ATM and of the transaction number in transit in respect of an authorization request shall be detectable.

OE.INT_CR Any modification of messages notifying the server of a modification of the cash balance in the ACD/ATM while they are being transferred within the telecommunication network shall be detectable.

OE.ACCEPT The AAC shall carry out or initiate the card acceptance checks appropriate to the technology of the card.

OE.MAINT People responsible for the ACDs/ATMs shall employ trusted maintenance staff and bank tellers.

OE.REN_CLES Encryption keys shall be renewed frequently.

Security Target I

- Set of security requirements and specifications used as the basis to evaluate a concrete ToE (e.g., Triton ATM RL2000, v3.7)

  Specifies what a (subset of a) concrete system should do

- ToE includes:
  - Security threats, objectives (e.g., determined by **O**rganizational **S**ecurity **P**olicy), and requirements
  - Assumptions on operational environment
  - Measures (**T**oE **S**ecurity **F**unctions) intended to counter threats
  - Determination of Evaluation Assurance Level

Security Target II

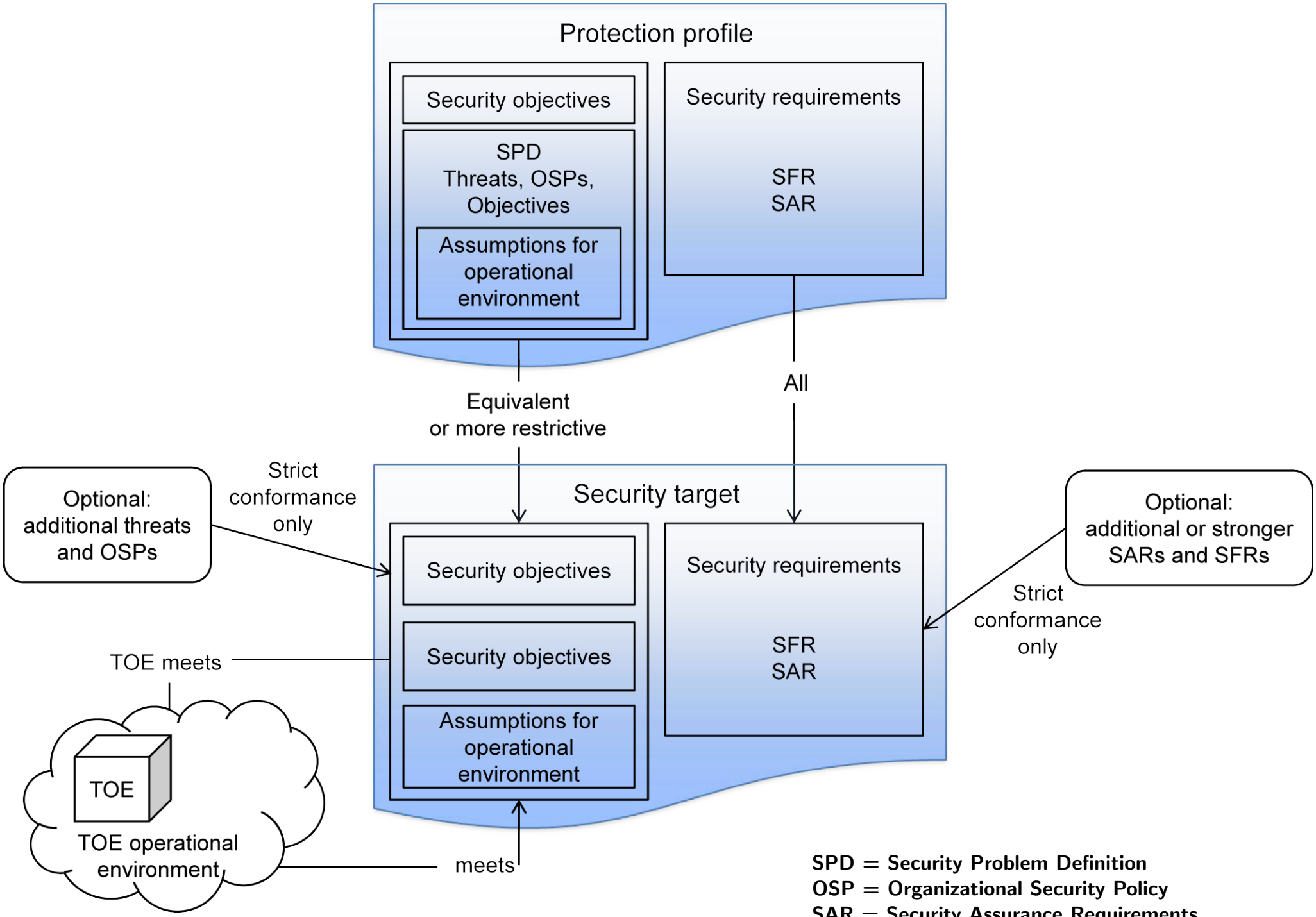
- Requirements derived by refining/instantiating one or more PPs
- Must be checked for completeness and lack of contradictions, i.e., are themselves evaluated (not said how this is done)
- Usually published so consumers know what was certified
- Interpretation of results is only possible with respect to ST.

  "Microsoft Windows XP Embedded with SP2" alone says little

General procedure

- Write/get Protection Profile
- Evaluate PP. Complete, consistent, technically sound?
- Write/get Security Target
- Evaluate ST. Complete, consistent, technically sound?
- If claimed: show conformance with PP
- Evaluate ToE with respect to given EAL. Show security requirements of ST are met

We expand on ST and EALs in parts II and III



SPD = Security Problem Definition
OSP = Organizational Security Policy
SAR = Security Assurance Requirements

Part 2: security functional requirements

- Specify TOE's expected security behavior in terms of behavior of ToE's individual **security functions**

- Behavior specified in terms of what users can detect by interacting with TOE (inputs/outputs) or TOE's response to environment

  Recall security testing: detect failures!

- ToE evaluation WRT enforcement of a **T**oE **S**ecurity **P**olicy (TSP)
  - Rules by which ToE governs access to its resources
  - Made up of security function policies with own scope of control
  - Implemented/enforced by **security functions**
    These are the parts of the ToE that must be relied on to enforce (a subset of) rules from the TSP

Security functional requirements

Security audit: record, store, analyze security relevant information

Communication: Non-repudiation of origin and receipt

Cryptographic support: key management and operations.

User data protection: access control, integrity, offline storage, ...

Identification and authentication

Security management: audit, revocation/expiration, role mgmt, ...

Privacy: anonymity, pseudonymity, unlinkability, unobservability

Protection of ToE security functions

Resource utilization: priority of service, resource allocation/limits

ToE access: sessions, access control

Trusted paths: between users and ToE security functions

Example: cryptographic support class

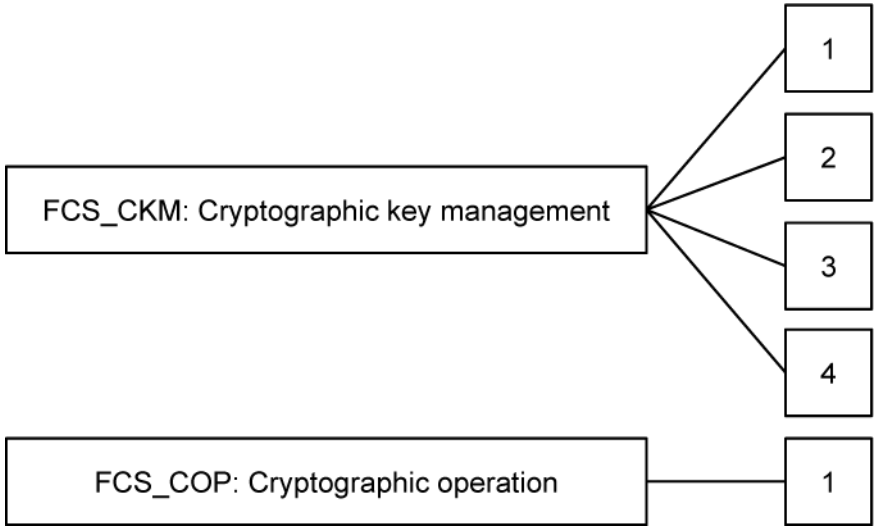
CKM1 Key generation

CKM2 Key distribution

CKM3 Key access

CKM4 Key destruction

COP1 Cryptographic operation



Example: FCS-CKM.1.1: The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment:*cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]

Assurance

- Goals
  - Ensure TSF (ToE Security Functions) correctly implemented
  - Ensure ToE can be installed and securely operated
  - Ensure ToE's integrity maintained during development and delivery

- Associated activities for different parties

  Developer: Configuration management, deliver and operation, development, tests, ...

  Evaluator: Tests, vulnerability analysis (of mechanisms), ...

TOE assurance requirements I

- **Configuration management**

  Automation, capabilities, scope

- **Delivery and operation**

  Delivery, installation, and start-up

- **Development** (ToE security functions only)

  Functional specification, high-level design, low-level design, implementation representation of ToE security functions, representation correspondence, security policy modeling

- **Guidance documents**

  Documentation for admins and users

TOE assurance requirements II

- **Life-cycle support**

  Development security, flaw remediation, life cycle definition

- **Tests**

  Functional tests, (functional) coverage, depth, independent testing

- **Vulnerability assessments**

  Covert channel analysis, misuse, strength of ToE security functions, vulnerability assessments

Assurance techniques

- Analyze processes and procedures. Ensure they are applied.
- Analyze correspondence between ToE design representations
- Analyze ToE design representation against requirements
- Verify proofs
- Analyze functional tests developed and results provided
- Independent functional testing
- Vulnerability analysis and penetration testing

Most of this is focused on product itself!

A first impression of EALs

- Extensive configuration management: $\geq$ EAL3
- Tool-based configuration management: $\geq$ EAL4
- Delivery processes: $\geq$ EAL2
- High-level design: $\geq$ EAL2
- Semi-formal development $\geq$ EAL5
- Formal methods: $\geq$ EAL7
- Security policy model: $\geq$ EAL4
- Formal security policy model: $\geq$ EAL5
- Test coverage: $\geq$ EAL2

EALs 1–2

EAL 1: Functionally tested

- Security threats not considered serious
- Independent testing against (vague) functional/interfaces specifications, not against high-level designs

EAL 2: Structurally tested

- Developer testing against (better) specification
- Vulnerability analysis
- Independent testing using more detailed ToE spec
- "Structured" refers to process, not structured testing per se

EALs 3–4

EAL 3: Methodically tested and checked

- More complete testing + coverage of security functions (Not structural coverage)
- Environmental controls such as version control and mechanisms/procedures to ensure that ToE not tampered with

EAL 4: Methodically designed, tested, and reviewed

- Specification/analysis of all interfaces
- High/low level design documentation + subset of impl.
- Improved mechanisms to ensure ToE not tampered with during development and delivery.
- "State-of-the-art" SW development processes (tool based, specification techniques), etc.

EALs 5–6

EAL 5: Semiformally designed and tested

- Semiformal design description required for entire implementation
- More structured architecture
- Covert channel analysis
- Improved mechanisms/procedures that provide confidence that the ToE will not be tampered with during development

EAL 6: Semiformally verified design and tested

- Semiformal design descriptions: restricted syntax language with defined semantics
- Structured representation of impl. which is more analyzable
- Improved configuration management and controls

EALs 7

EAL 7: Formally verified design and tested

- Comprehensive analysis using formal representations and formal correspondence.
  I.e., well-defined syntax and semantics using well-established mathematical concepts
- Comprehensive testing

EAL4 is typical — here in more detail

- Complete interface specification
- Analysis extended to implementation level (subset of source code)
- Informal security policy model
- Documentation of developer's tests (functional specification and high-level design)
- Independent testing of (sample of) security functions
- Strength-of-function analysis (how much effort is required to defeat ToE security functions)
- Vulnerability analysis by developer
- Independent vulnerability analysis
- Configuration management automation
- Secure delivery procedures

EALs mapped onto classes (higher numbers indicate greater strength)

Assurance class	Assurance family	Assurance components by evaluation assurance level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	1	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Summary CC

- Structured catalogs of security-relevant requirements
- Description of how to assure these requirements

  Different strengths: EALs
- No international agreement on (and need to trust) EAL > 4 yet
- Huge list of protection profiles: reuse!
- Huge list of evaluated products
- Empirical studies?
- CC established, among others, in smartcard domain

  E.g., Austrian digital signature law requires CC certification

CC Pros

- Focus on product!
- No hard guarantees, but system must pass a thorough evaluation

  $\Rightarrow$ substantially increased confidence in its security
- Transparency: PPs provide overview of issues for product classes and EALs elaborate assurance options
- It is standard/required by numerous industries and governments

  Smart card operating systems, digital signature platforms, military systems, ...
- Wide acceptance: no need for re-certification in different countries

CC Cons

- TOE is one particular version of a system

  Except for minor changes (flaw remediation), changes require complete re-evaluation; particularly so when security is involved

- Timing: systems age quickly. CC-certified product up-to-date?

- Lots of jargon and terrible acronyms!

- No notion of cost-effectiveness

- Quality of PPs? Don't accept blindly!

Road map

- Motivation
- NIST
- ISO/IEC 27000 series
- Common Criteria

☞ **BSI baseline protection (Grundschutz)**

- Conclusions

BSI[3] IT Baseline Protection (IT Grundschutz)

Many security issues are common to many applications and organizations. Can we reuse knowledge of general solutions?

- **Baseline protection**: catalog of relevant issues for most systems
  - Components of an IT system
  - List of associated threats
  - List of associated safeguards
- Applies just to standard system components
- Qualitative risk analysis + corrective measures

[3] German Bundesamt für Sicherheit in der Informationstechnik

BSI standards and recommendations

BSI Standard 100-1: General requirements for an ISMS. Compatible with ISO 27001.

BSI Standard 100-2: IT-Grundschutz Methodology: Concretizes 100-1: explains in detail how to produce a "security concept", select safeguards, and monitor progress.

BSI Standard 100-3: Risk analysis based on IT-Grundschutz. Methods for risk analysis and determining when security requirements go beyond "normal" measures.

BSI Baseline Protection Catalog: Very comprehensive IT Security guide (4,000+ pages). Contains guidelines for securing and evaluating typical systems built from standard technologies.

Idea (high-level)

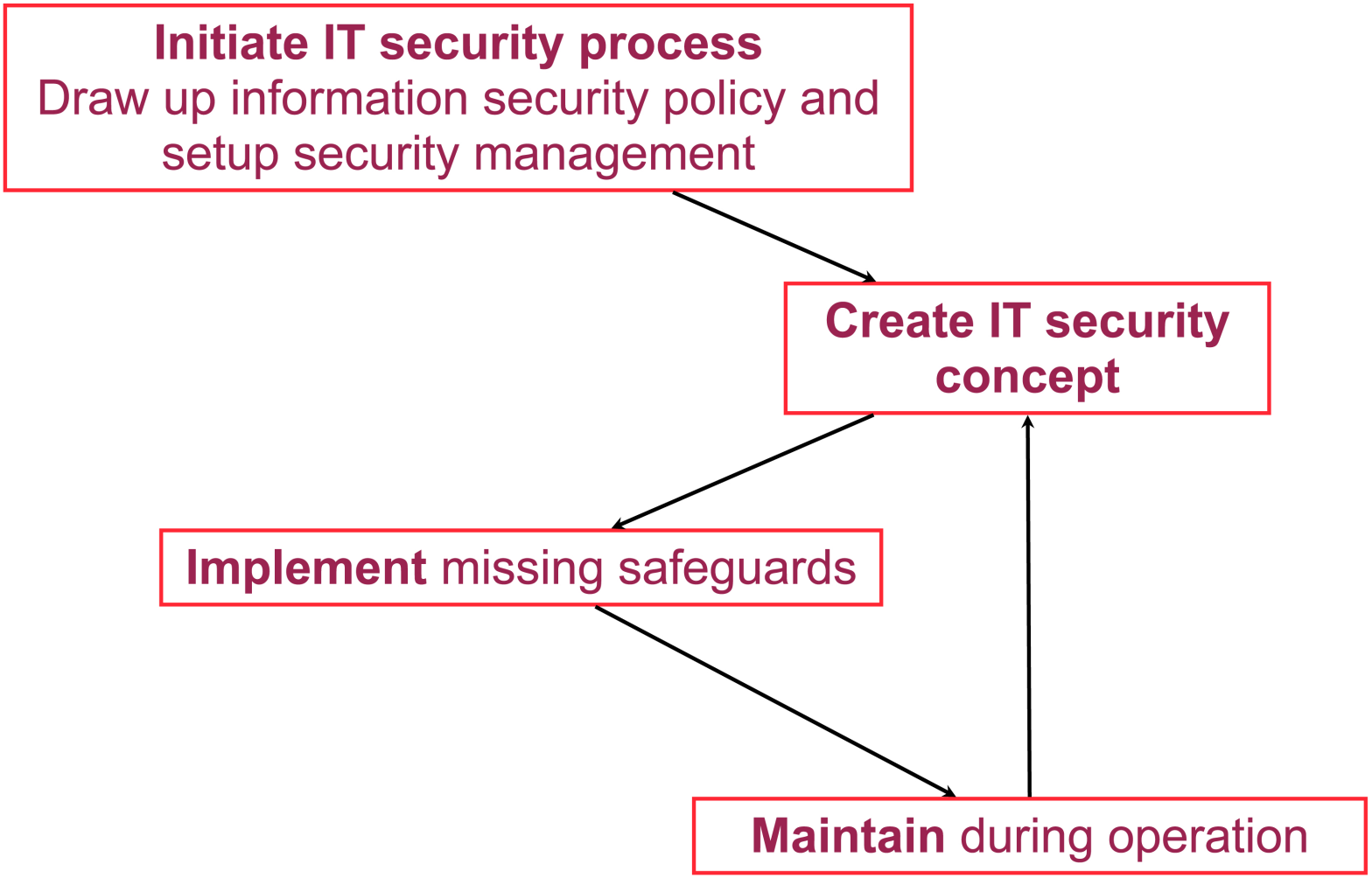
- Apply **standard measures in normal cases**
  - Replace risk analysis (likelihood, impact, safeguard) by a guided comparison of current and recommended safeguards
  - Afterwards, implement any missing safeguards
- Perform a dedicated **risk analysis only in extreme cases**

  Additional analysis and safeguards only when dictated by significantly higher security requirements
- By concentrating on standard technologies, detailed and up-to-date recommendations are possible

  And typical systems are mostly standard, anyway

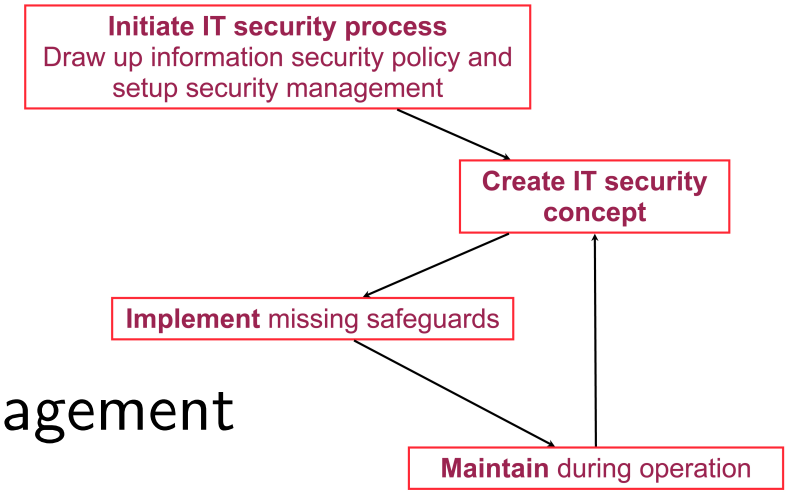
Pragmatic approach based on standard problems and solutions

Associated security process



We present just a few highlights

Initiate Security Process



- Management accepts responsibility

  Security management as part of risk management

- Design and plan the security process

  Process should support continual risk analysis, linked to business/security objectives

- Create an information security policy

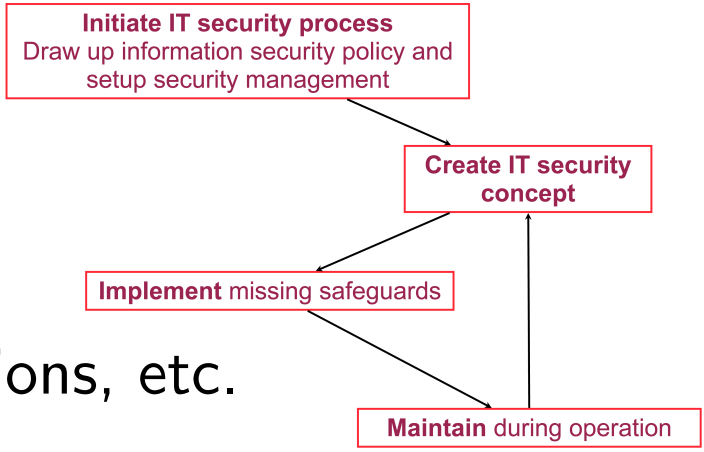
  Concise statement of scope, target, and key objectives

- Establish an organization structure for security management

- Provide financial resources, personnel, necessary time

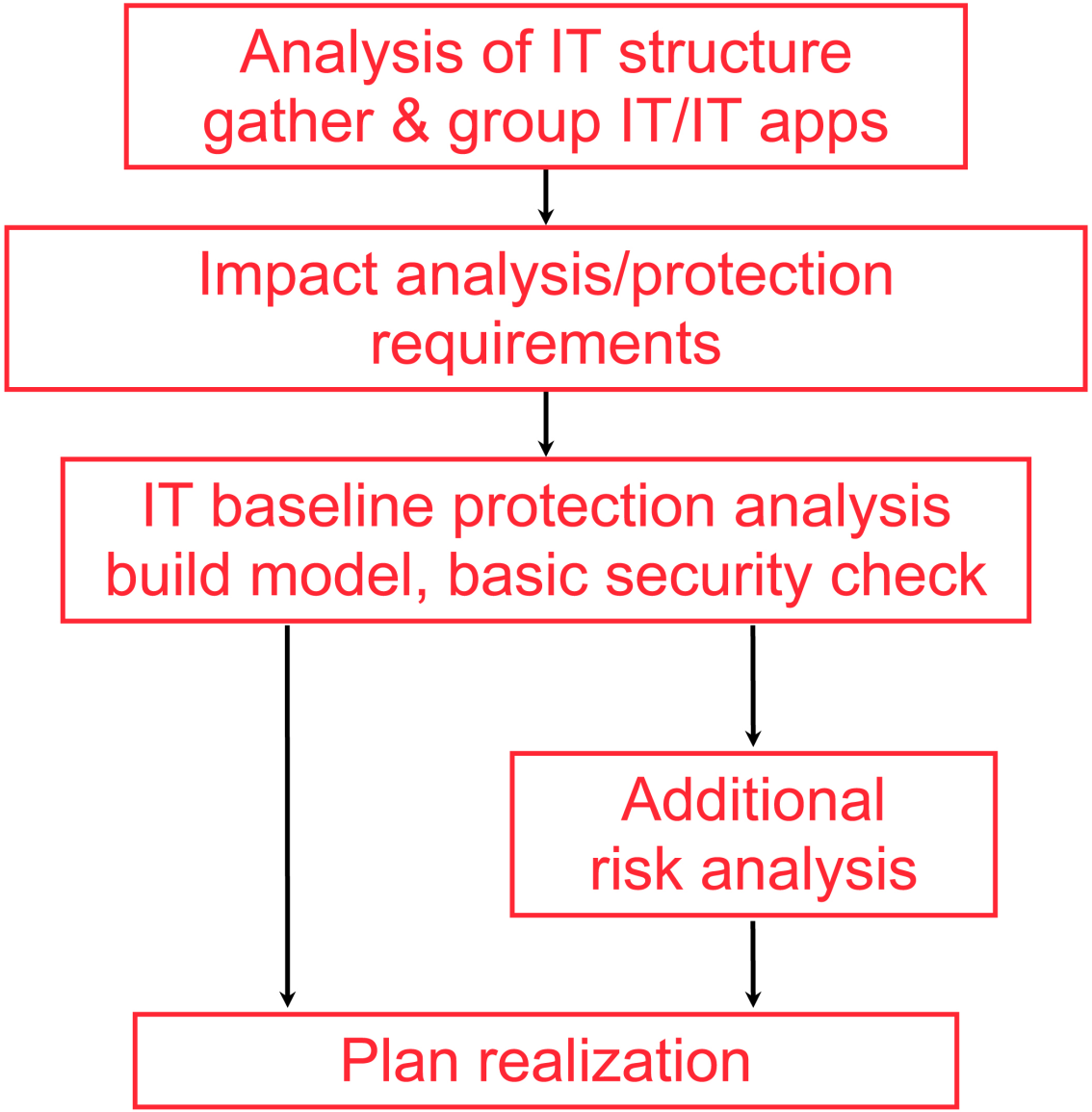
- Integrate all relevant employees (training, reporting ...)

Create IT Security Concept

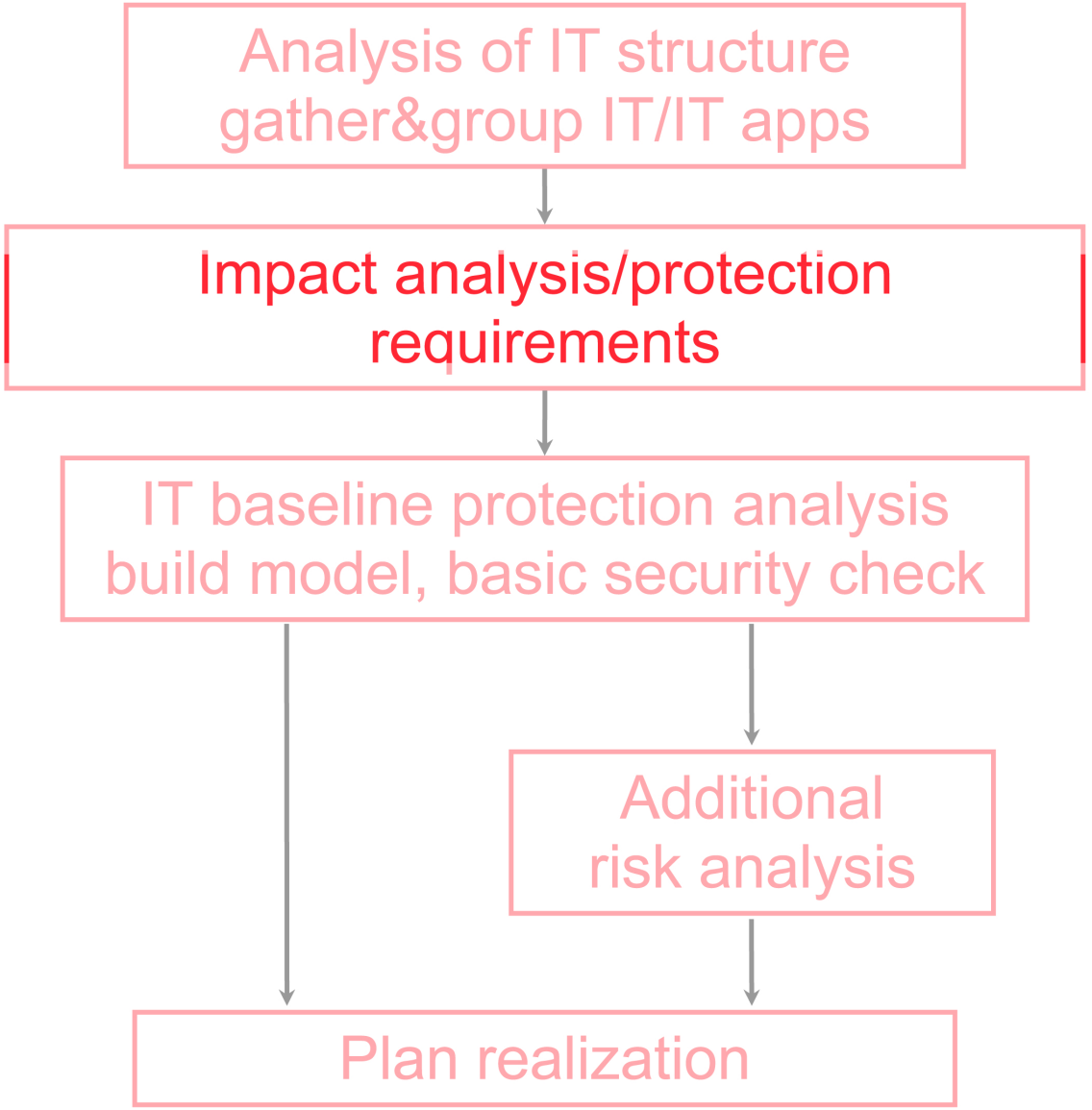


- Determine existing IT structure: IT systems applications, networking equipment, connections, etc.
  - Typical starting point: a network topology plan
  - Group objects of same type/configuration, e.g., Windows PC
  - List in tabular form along with protection requirements (CIA)
- Identify also non-technical infrastructure, e.g., personal
- Map elements (technical and organizational) of current/intended IT structure to manual's modules
- Dedicated risk analysis for assets with high security requirements and for non-standard components
- Compare current situation to recommended safeguards and take actions where necessary

Create IT Security Concept — steps



Create IT Security Concept



Impact analysis
Similar to other risk analysis methodologies

- Determine impaired performance of duties
  - Violation of laws, regulations or contracts
  - Impairment of informational self-determination
  - Negative effects on external relationships
  - Financial consequences
- Damage scenarios via "what if" questions for loss of CIA
  - Reflect different viewpoints: user, legal, etc.
  - E.g. is confidentiality of data required by law?
- Goal: determine degree of necessary protection in terms of CIA

  Particularly sensitive assets are later given an extra risk analysis

Impact categories

- **Normal (basic to moderate)**
  - Violations of regulations, laws, contracts with minor consequences.
  - Acceptable costs, loss of reputation, etc.
- **High**
  - Violations of regulations, laws, contracts with major consequences.
  - Possible injury to individuals (physical or through loss of data).
  - Considerable harm to reputation.
  - Substantial financial loss, but enterprise would survive it.
- **Very high**
  - Fundamental violation of regulations or contracts with ruinous liabilities.
  - Misuse of personal data could mean financial ruin for involved party.
  - Serious injury to individuals is possible.
  - Nation-wide loss of reputation. Possibly endangering enterprise.
  - Sever financial losses, possibly endangering enterprise.

Combination of requirements

IT systems aggregations assets — requirements for systems?

- **Maximum principle**

  Protection requirement of an IT system determined by damage or sum of most serious instances of damage

- **Dependency relationships**

  Protection of A itself is low, that of B high, B uses output of A: increase protection requirements of A

- **Cumulative effects**

  Different applications run on one server; each of them with low protection requirements; servers crash would do harm

- **Distributive effect**

  Only irrelevant parts of a "high" application run on a server; server hence not necessarily with high protection requirements

Combination examples

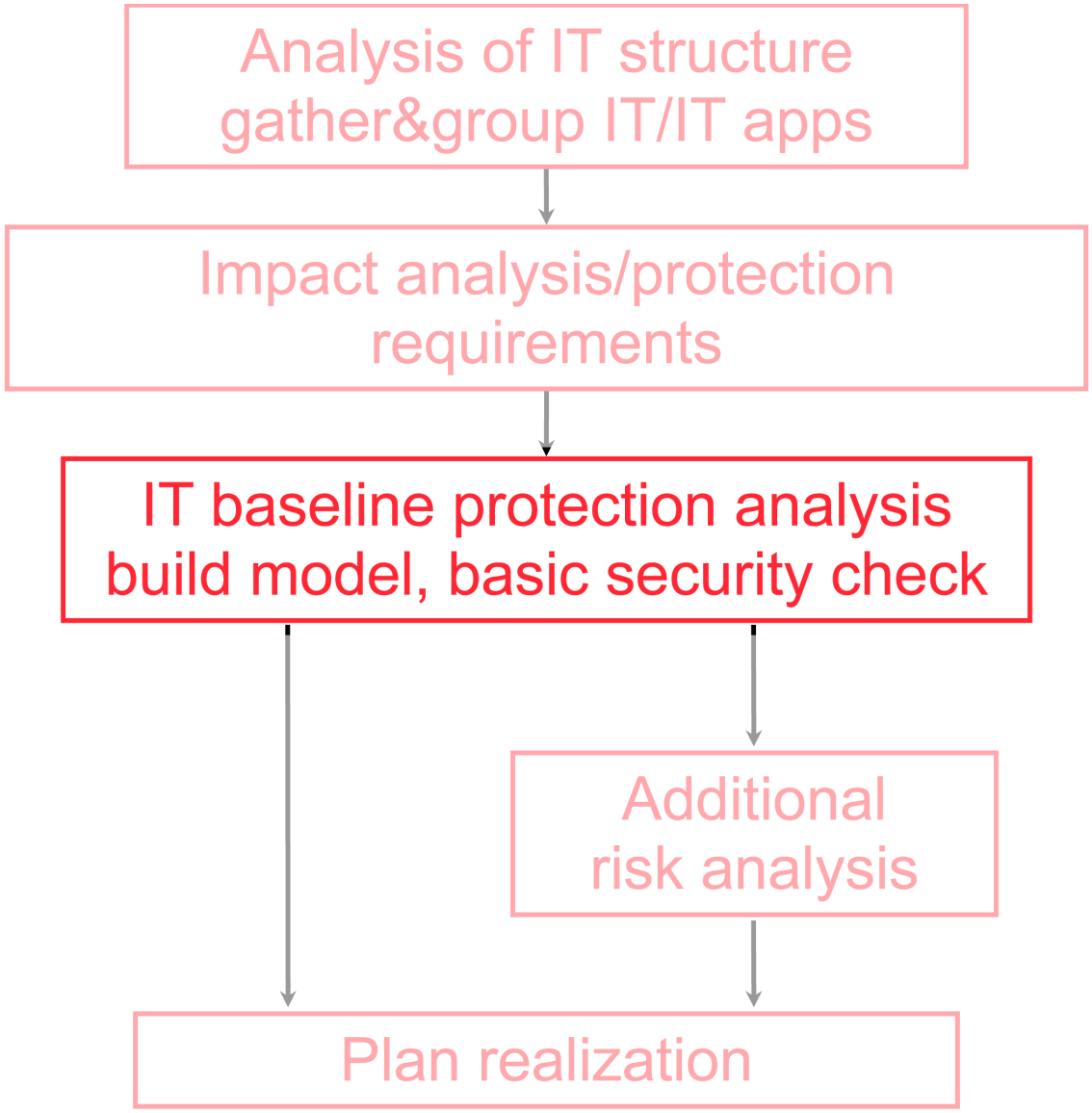
- **Example of cumulative effect**

  All applications processing customer data are located on one network server. Damage in the event of an application failure is estimated to be low since there are alternatives. However if the server fails (and therefore all applications) then estimated damage is considerably higher.

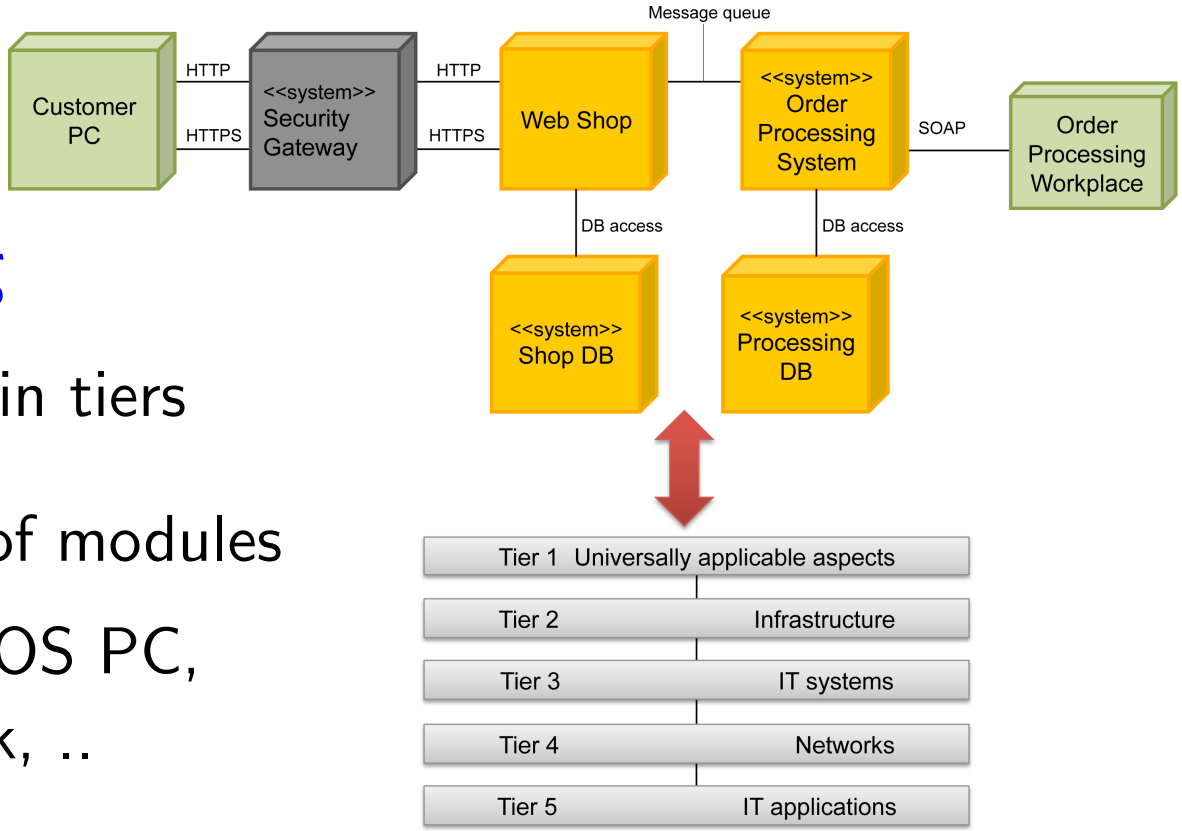
- **Example of distributive effect**

  If an IT system has been designed to be redundant, the protection requirements of individual components may be lower than the requirement of the entire application. Redundancy in general is a common source of distributive effects.

Create IT Security Concept



Core activity infrastructure mapping



- Baseline catalog organized in tiers
- Each tier consists of a set of modules

  Examples: server room, DOS PC, firewall, web server, outlook, ..
- Map enterprise infrastructure, including personal, buildings, etc., onto modules
- For each of the modules, check threats and safeguards

  Compare current and recommended safeguards
- For specialized protection requirements, perform dedicated risk analysis

Domain concepts — tiers

1. **Generic IT security aspects**

   Security management, organization, backup, outsourcing

2. **Infrastructure**

   Building, cabling, server room, cabinets, mobile workplace.

3. **Individual IT systems (may be grouped together)**

   Windows NT servers, Unix clients, routers, fax

4. **Network**

   Network and system management, firewalls, remote access

5. **Actual IT applications**

   E-mail, Lotus Notes, Apache Web Server, databases

Components I — Generic

- Security management
- Organization
- Personnel
- Contingency planning
- Data backup policy
- Data privacy protection policy
- Computer virus protection
- Cryptographic concept
- Handling of security incidents
- Hardware and software management
- Outsourcing

Each of these is related to a set of threats and safeguards

Components II — Infrastructure

- Buildings
- Cabling
- Office (both workplace and home office)
- Server room
- Data media archives
- Technical infrastructure room
- Protective cabinets
- Computer centers

Components III — (Non)Networked systems

- Non-networked
  - DOS/Windows systems: single/multi user, client/server
  - Unix systems
  - Laptops
  - Internet PCs (not connected to the Intranet)
- Networked
  - UNIX/Windows-based
  - Novell
  - Heterogeneous networks

Components IV — Data transmission, etc.

- Data transmission

  Data media, modem, firewall, e-mail, web servers, remote access, Lotus Notes, Exchange/Outlook

- Telecommunication

  Telecommunications systems (private branch exchange), fax machine, answering machine, LAN integration via ISDN, fax server, mobile telephones

- Standard software, data bases, telecommuting, archiving

Threats and safeguards

Threat Catalog

- 14 Force majeure
- 97 Organizational shortcomings
- 63 Human failure
- 44 Technical failure
- 111 Deliberate acts

Safeguard Catalog

- 60 Infrastructure
- 275 Organization
- 37 Personnel
- 200 Hardware and software
- 110 Communication
- 90 Contingency planning

Combined in tables

(here for mobile workplace)

Safeguard/threat	T2.47	T2.48	T 3.3	T3.43	T3.44	T5.1	T5.2	T5.4
S1.15						X		X
S1.23						X		X
S1.45	X	X					X	X
S1.46							X	

An example: wireless LAN

Threat Scenarios

The following typical threats to the IT-Grundschutz of WLAN usage are assumed to exist:

Force majeure:

- T 1.17 Failure or malfunction of a wireless network

Organizational shortcomings:

- T 2.1 Lack of, or insufficient, rules
- T 2.2 Insufficient knowledge of rules and procedures
- T 2.4 Insufficient monitoring of IT security safeguards
- T 2.117 Lack of, or inadequate, planning of the use of WLAN

Human error:

- T 3.3 Non-compliance with IT security safeguards
- T 3.9 Improper IT system administration
- T 3.38 Errors in configuration and operation
- T 3.43 Inappropriate handling of passwords
- T 3.84 Incorrect configuration of WLAN infrastructure

Technical failure:

- T4.60 Uncontrolled radiowave propagation
- T4.61 Unreliable or missing WLAN security mechanism

Deliberate acts:

- T 5.71 Loss of confidentiality of classified information
- T 5.137 Analysis of connection data relating to wireless communication
- T 5.138 Attacks on WLAN components
- T 5.139 Tapping of WLAN communication

Recommended safeguards
A series of security safeguards must be implemented when using WLAN, starting in the conception phase and continuing through the purchasing phase to the operation phase.

Planning and design
The securing of a WLAN begins already in the planning phase. A foundation for a secure WLAN can only be created through a well thought out strategy (see S 2.381 *Determining a strategy for the use of WLAN*) and the selection of the correct WLAN standards, and therefore of the corresponding cryptographic method (see S 2.383 *Selection of a suitable WLAN standard* and S 2.384 *Selection of suitable crypto-methods for WLAN*). The safeguard S 3.58 *Introduction to WLAN basics* will help you become familiar with the terminology used when describing how to secure a WLAN.

All decisions made relating to security settings, the WLAN standards selected, as well as the rules for the use and administration of the WLAN are to be written down in a WLAN security policy (see S 2.382 *Drawing up a security policy for the use of WLAN*).

Procurement
When selecting the WLAN components, safeguard S 2.385 *Selection of suitable WLAN components* must be applied. The standards, protocols, and security mechanisms used in WLANs are subject to rapid development, which is why WLANs are often in the middle of a migration.

Safeguard S 2.386 *Careful planning of necessary WLAN migration steps* must be taken into account for the migration phases of individual WLAN components or entire sections of the WLAN.

Planning and design

- S 2.381 (A) Determining a strategy for the use of WLAN
- S 2.382 (A) Drawing up a security policy for the use of WLAN
- S 2.383 (A) Selection of a suitable WLAN standard

Procurement

- S 2.385 (A) Selection of suitable WLAN components
- S 2.386 (A) Careful planning of necessary WLAN migration steps

Implementation

- S 1.63 (B) Appropriate location of access points
- S 2.387 (A) Installation, configuration, and support service for a WLAN by third party
- S 3.59 (C) Training on the secure use of WLAN
- S 4.294 (A) Secure configuration of access points
- S 4.295 (A) Secure configuration of WLAN clients
- S 5.139 (A) Secure WLAN-LAN connection
- S 5.140 (C) Setting up a distribution system

A = essential, B = needed for certification, C = recommended but optional

Summary — mapping

- Standard 100-1 gives more detail on building IT-infrastructure model

  Our models could also serve as a starting point

- Mapping components onto modules from protection catalog yields standard threats and safeguards (when components also standard)

- If sufficient safeguards are in place: test them!

- If safeguards are lacking: develop plan, implement, and then test!

- Approach comparable to ISO 27000 series

  However, BSI approach makes standard threats/safeguards explicit

Road map

- Motivation
- NIST
- ISO/IEC 27000 series
- Common Criteria
- BSI baseline protection (Grundschutz)

☞ **Conclusions**

Strengths of standards and certification

- Standards distill best practices into guidelines and processes
- Key benefits
  - They help to approach the problem in a structured way
  - They get key players involved, e.g., management
  - Certification documents your efforts to others
- Additional benefits
  - They raise awareness and bring about positive changes
  - They define a benchmark to aim for
- For large enterprises there are not many viable alternatives

Weaknesses

- Results of a certification audit depend strongly on auditor

  Honesty, objectivity, knowledge and experience, thoroughness

- Many auditors replace technical knowledge with check-lists

  "Do you have water pipes in your server room?"

- Concrete limitations must also be understood
  - **Example ISO 27001:** Drafting security policies and training employees doesn't ensure employees correctly follow procedures
  - **Example CC:** specification may be incomplete or wrong, testing and analysis only partial, ...

- **In general:** Compliance $\not\Leftrightarrow$ Security

Literature

- NIST publications
  csrc.nist.gov/publications/PubsSPs.html
- Common Criteria, www.commoncriteriaportal.org
- ISO/IEC 27000 standards, www.iso.org and
  http://www.27000.org
- BSI Resources, www.bsi.bund.de.
- Mikko Siponen, *Information Security Standards Focus on the Existence of Process, Not Its Content*, Communications of the ACM, August 2006.