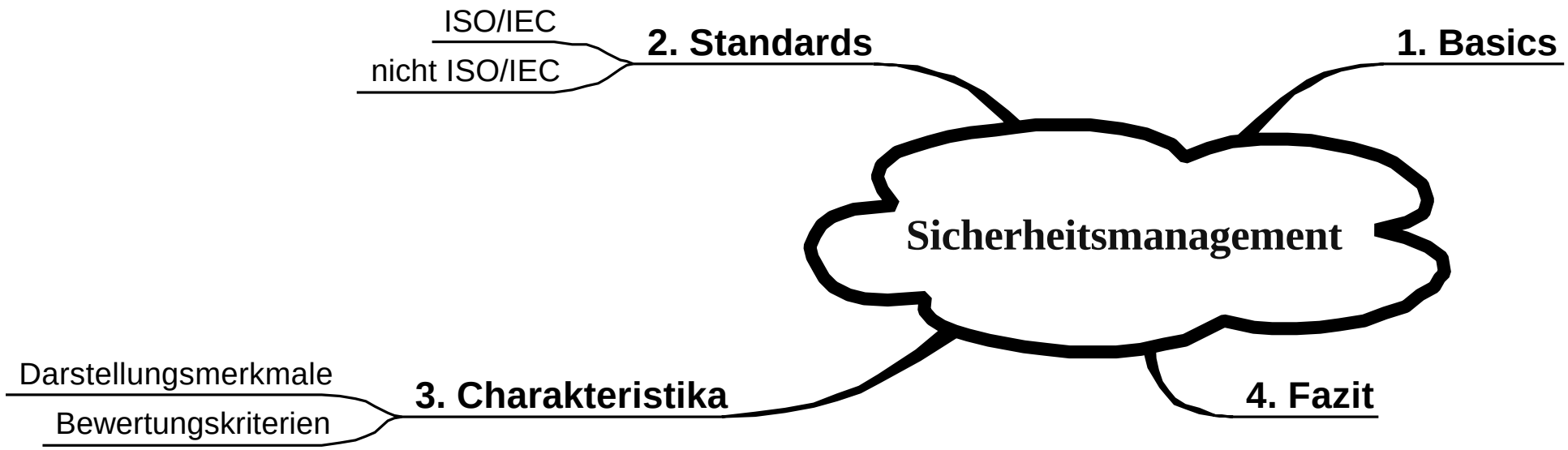
Nachweis der erreichten Sicherheit durch Prüfungen nach Standards?!

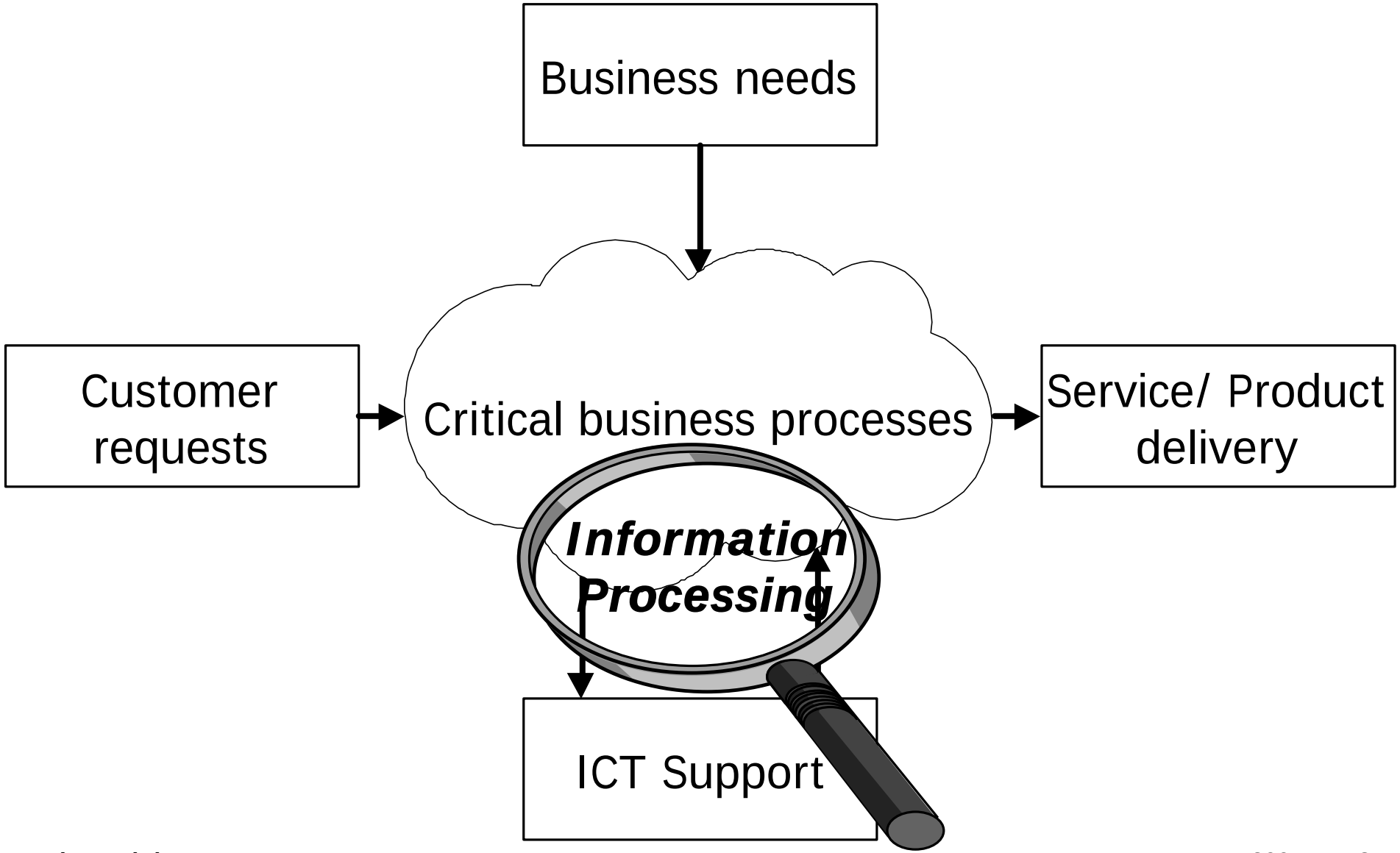
DECUS Rheinlandtreffen

St. Augustin, 18.11.2004

Bundesamt für Sicherheit in der Informationstechnik


ISO/IEC
nicht ISO/IEC
2. Standards
1. Basics
Sicherheitsmanagement
Darstellungsmerkmale
Bewertungskriterien
3. Charakteristika
4. Fazit

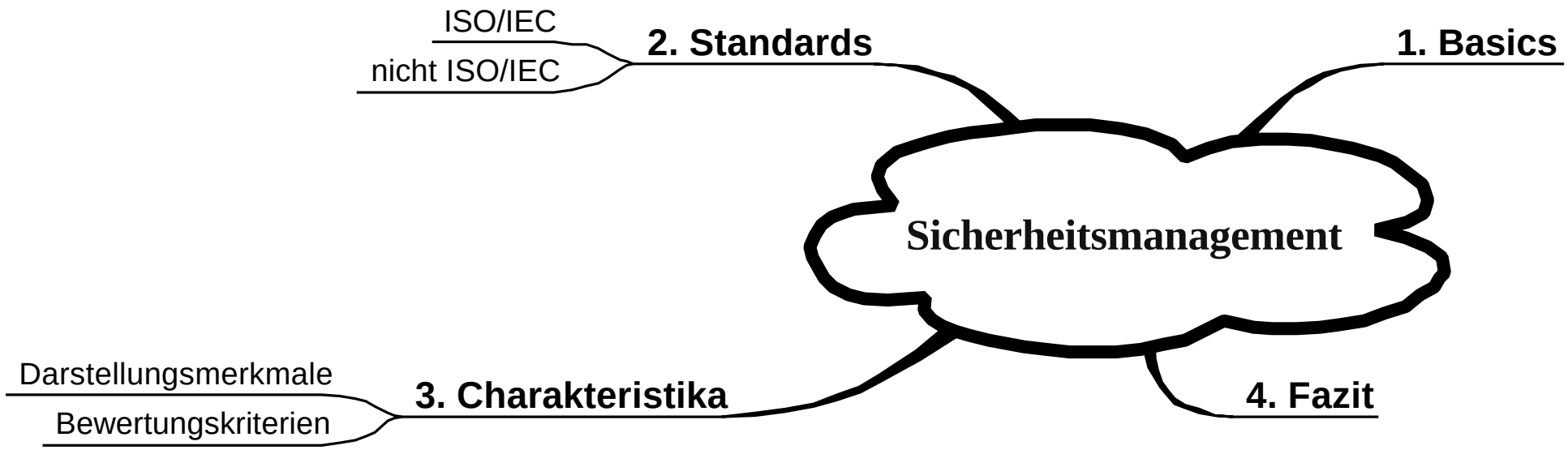
Securing business processes



Relationship between I and ICT

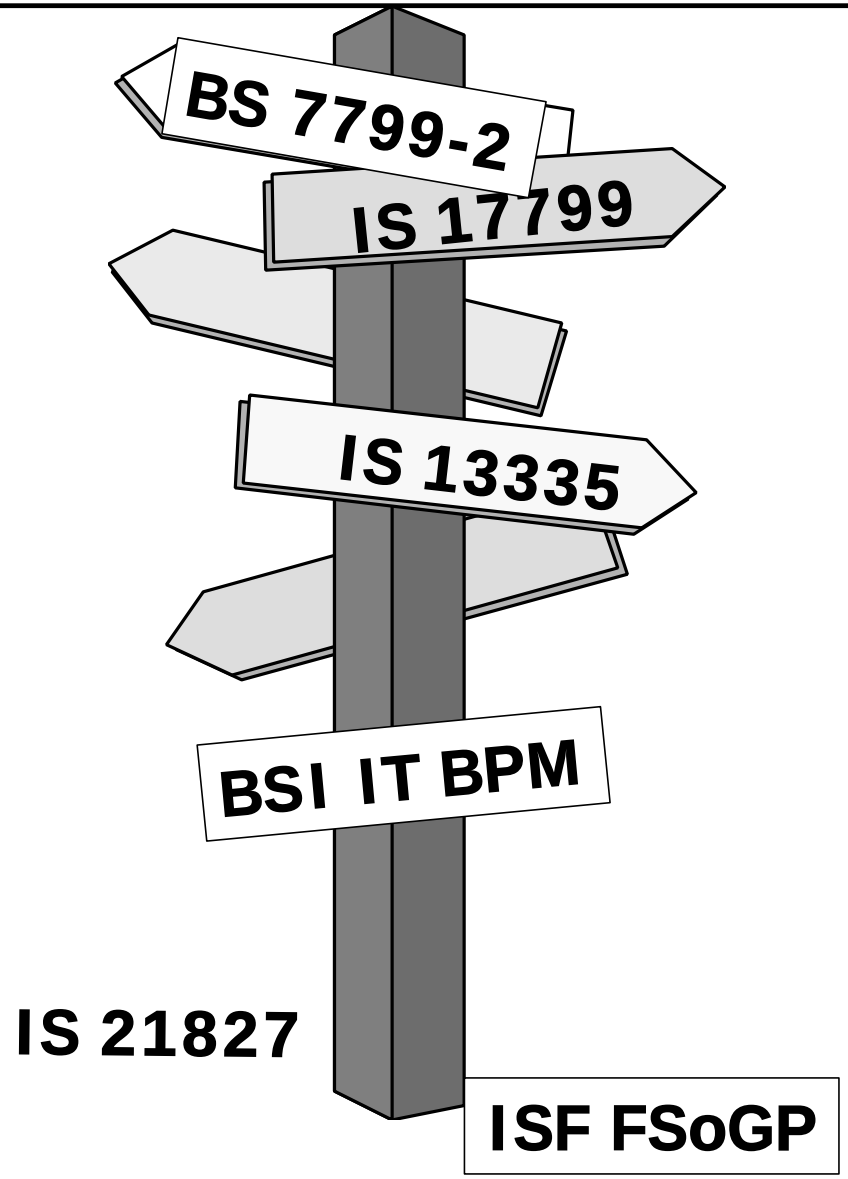
The more *Information* is processed by
Information and communications technology

the more *ICT Security* is required to secure *Information* !


ISO/IEC
nicht ISO/IEC
2. Standards
1. Basics
Sicherheitsmanagement
Darstellungsmerkmale
Bewertungskriterien
3. Charakteristika
4. Fazit

Bundesamt
für Sicherheit in der
Informationstechnik

Standard will guide you on your way



ISO / IEC-Standards on Security Management

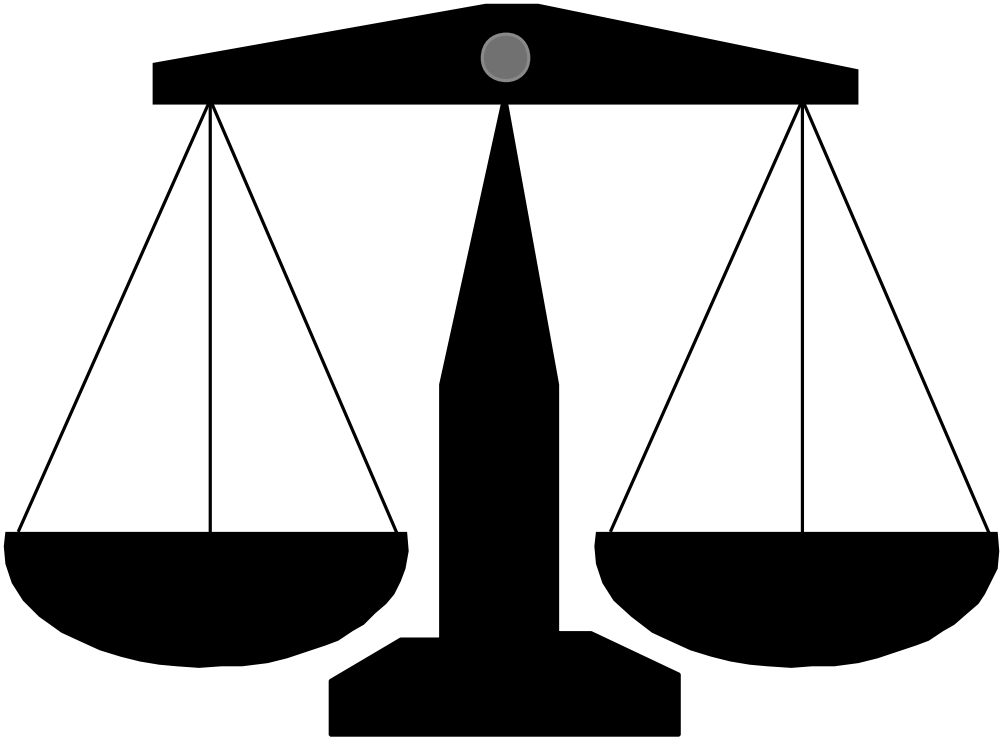
- ➔ TR 13335: Guidelines for the Management of IT Security (GMITS)
- ➔ *IS 13335: Management of information and communications technology security (MICTS)*
- ➔ *IS 17799: Code of Practice for Information Security Management*
- ➔ IS 21827: System Security Engineering - Capability Maturity Model
- ➔ TR 13569: Banking and other financial services
- ➔ ----------
- ➔ Study period on information security management systems
- ➔ =>
- ➔ *NP on ISMS requirements (IS 24743)*
- ➔ NP on ISM metrics and measurement (IS 24742)

Some more non ISO-Standards

- ➔ *(German) IT Baseline Protection Manual (IT BPM)*
- ➔ *(British) ISMS - Specification with Guidance for Use (BS 7799-2)*
- ➔ ----------
- ➔ ISF: The Forum's Standard of Good Practice (FSoGP)
- ➔ ISACA: Control objectives for information and related technologies (Cobit)
- ➔ NIST: An Introduction to Computer Security - The NIST Handbook (SP-800-12)
- ➔ ----------
- ➔ Information Technology Infrastructure Library (ITIL)
- ➔ ...

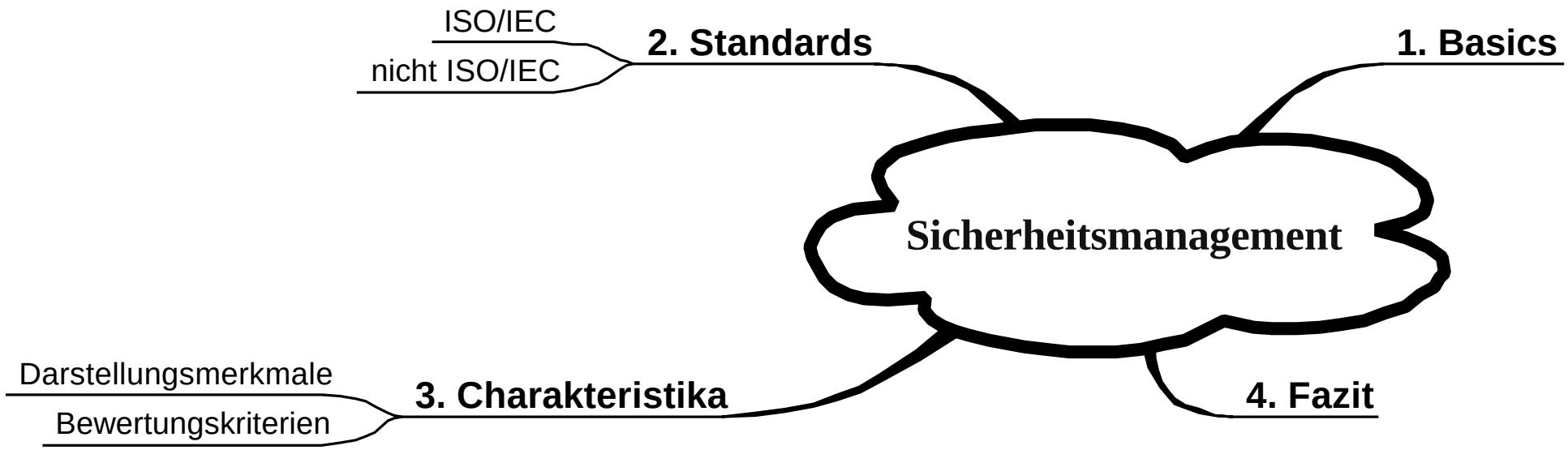
Benefit and effort of assessment

What a
standard
is able
to do!



What a
standard
is expected
to do!

Peer-to-peer comparison makes no sense
-> classification scheme


ISO/IEC
nicht ISO/IEC
2. Standards
1. Basics
Sicherheitsmanagement
Darstellungsmerkmale
Bewertungskriterien
3. Charakteristika
4. Fazit

Using which standard what for?

➔ Peer-to-peer comparison makes no sense
-> classification scheme

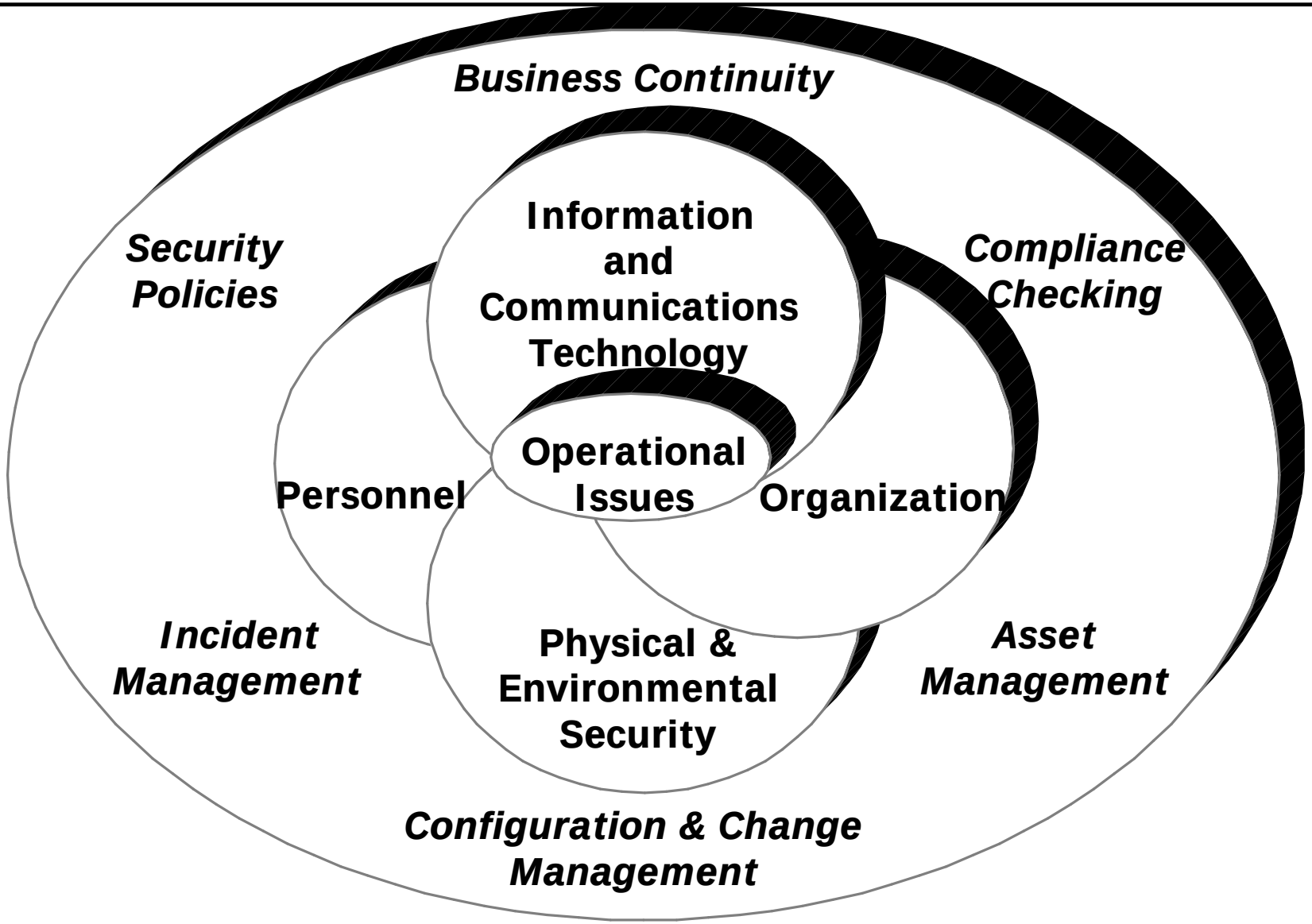
➔ ***„Black box“ comparison***
➔ ***-> characteristics: subject, audience, granularity, certificate***
➔ ***standard fits to users‘s problem***

➔ „White box“ comparison
➔ -> characteristics: purpose, focus, statement
➔ application of standard supports user‘s intention

IS 17799

- **“Code of practice for information security management”**
  (fast track of BS 7799-1, under revision since 2000, now FDIS)
- “… guidelines and principles for initiating, implementing, maintaining, and improving information security management …”
  -> what to do
  -> security officer
- … each area introduced by a description of the goal (“objective”) and structured into subchapters (“controls”) with different depth
  new: *control statement, implementation guidance, other information*
  … covers several control areas such as policy, organization, asset management, personnel, physical security, operational issues, access control, systems aquisistion & development, *incident management*, business continuity, and compliance
  new: *risk assessment and treatment*
- checklist without priority/ sequence
  BUT: no metric defined in order to support the assessment

17799 - Control areas

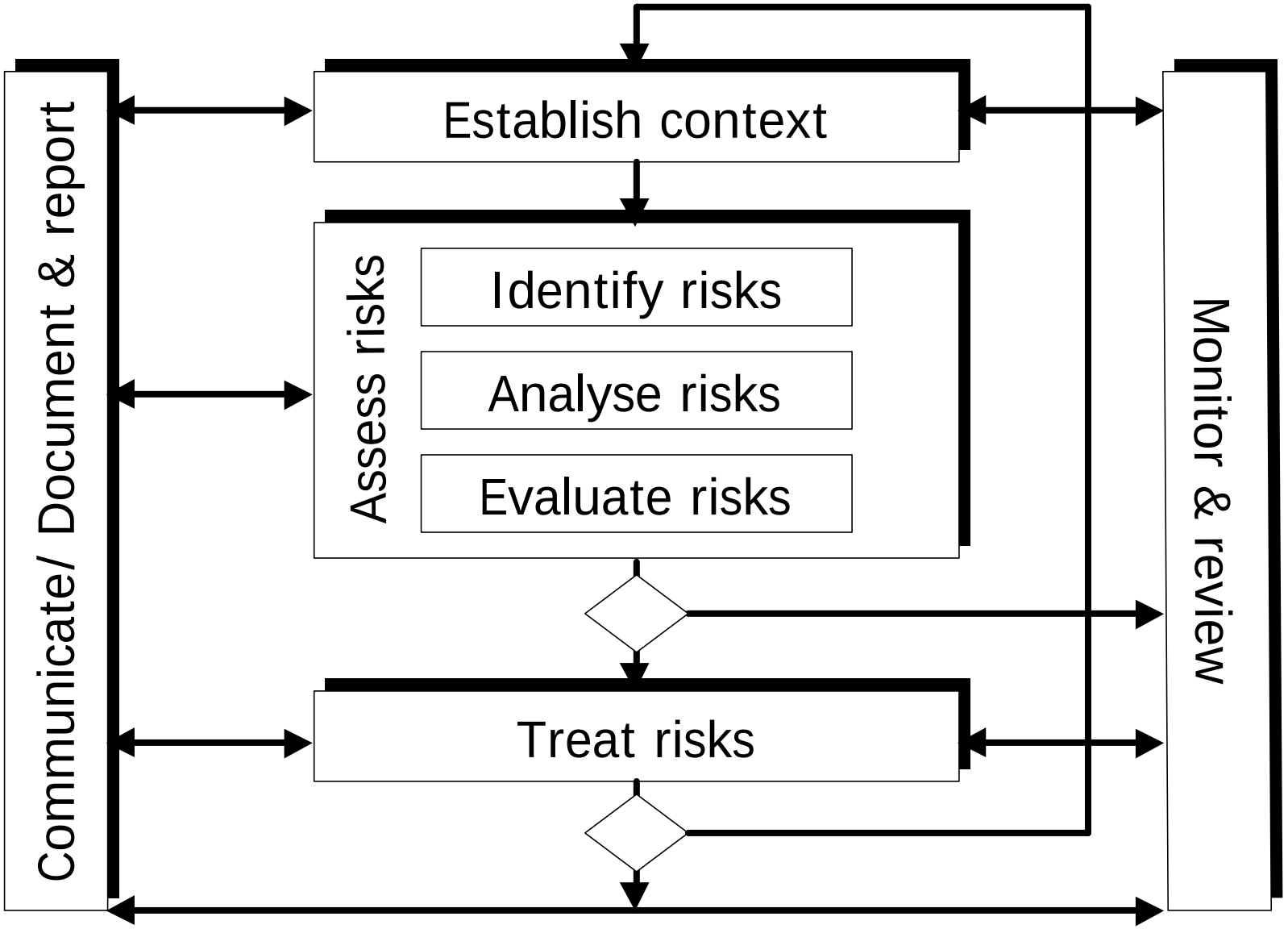


[See IS 17799]

IS 13335

- **“Management of Information and Communications Technology Security”** (MICTS = the “new” GMITS)
  part 1: concepts and models for ICT security management (now IS)
  part 2: techniques for ICT security risk management (now 4thWD)
- “… to assist the implementation of information security …”
  -> how to do
  -> security officer
- … covers security elements and relationships, ICT policy, organizational aspects, security management functions, risk management process
  … contains techniques for ICT risk management which can be used to assess security requirements and risks, and help to initiate and follow-up appropriate safeguards
- concepts/models, and techniques without pre-scribing
  BUT: no metric defined to check whether the techniques are “in place”

13335 - Risk activities



[See IS 13335-2]

BS 7799-2

- **“Information security management systems - Specification with guidance for use”**
  (new NP in ISO/IEC, now FCD)
- … based on the PDCA-model (by Deming)
  -> management system
  -> senior management
- …defines key elements such as general requirements, establishing an maintaining ISMS, documentation requirements, management commitment, resource management, general review requirements, review input, review output, internal audits, continual improvements, corrective and prevention action
  … emphasises systematic approach to risk assessment
- mingles operative and management processes
  BUT: no parameters/ indicators to “measure” effectiveness/ performance

IT BPM

- ➔ **“IT Baseline Protection Manual”**
- ➔ … focuses on ICT security
  -> what AND how to do
  -> security officer and administrator
- ➔ … based on the risk assessment methodology and risk treatment option of IS 13335
  … comprises criteria to select safeguards based on typical technical components & methodology to evaluate security level
  (based on a published assessment scheme)
  … deals with security activities/ elements supported by in-depth implementation guidance & gives background information on threats/ vulnerabilities listed in catalogues
- ➔ AND: defines metric to support assessment and to check whether techniques are “in place”

IT BPM - assess risks

Identify risks

IT Structure analysis:
Document technical topology (network plan)
Draw up inventory of assets (systems/applications)
Reduce complexity (by grouping)

Analyse risks

Analysis of protection requirements

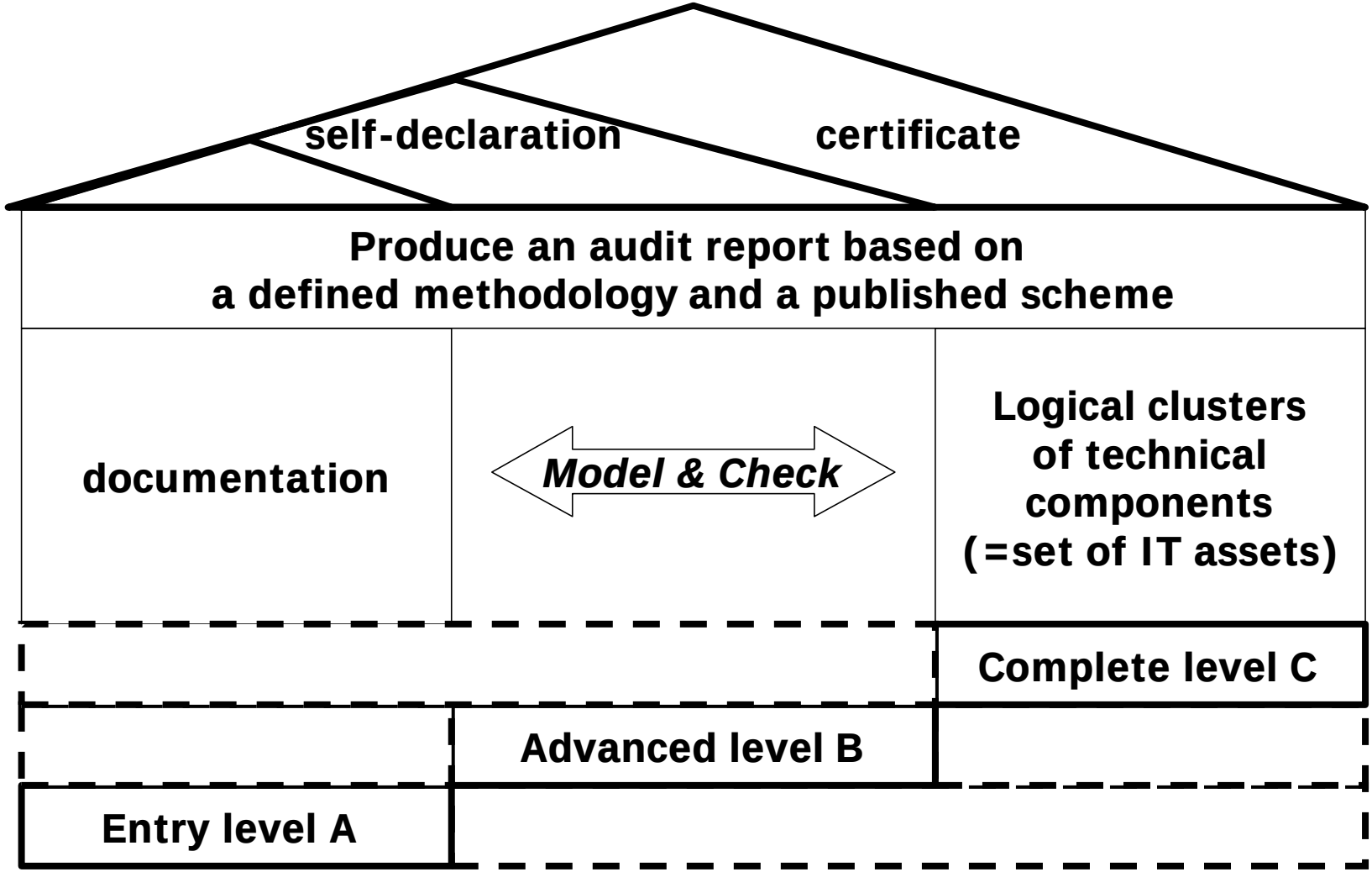
Baseline protection modelling

Supplementary security analysis

Evaluate risks

Security (compliance) checking:
Compare implementation against catalogues
Evaluate non-conformities
Document results

IT BPM - assessment



Black box comparison - summary

	subject	audience	granularity	certificate
IS 17799	Information Security	Security officer	Medium	No
IS 13335	Informations- & communications technology security	Security officer	Medium	No
BS 7799-2	Information Security	Senior management	Low	Yes
BSI IT-BPM	Informations- & communications technology security	Security officer & administrator	High	Yes

Using which standard what for?

➔ Peer-to-peer comparison makes no sense
-> classification scheme

➔ „Black box“ comparison
➔ -> characteristics: subject, audience, granularity, certificate
➔ standard fits to users‘s problem

➔ ***„White box“ comparison***
➔ ***-> characteristics: purpose, focus, statement***
➔ ***application of standard supports user‘s intention***

Sicherheitsmanagement ist ...

➔ die Gesamtheit aller ***Tätigkeiten*** und ***Zielsetzungen***

➔ zum Erreichen und Aufrechterhalten

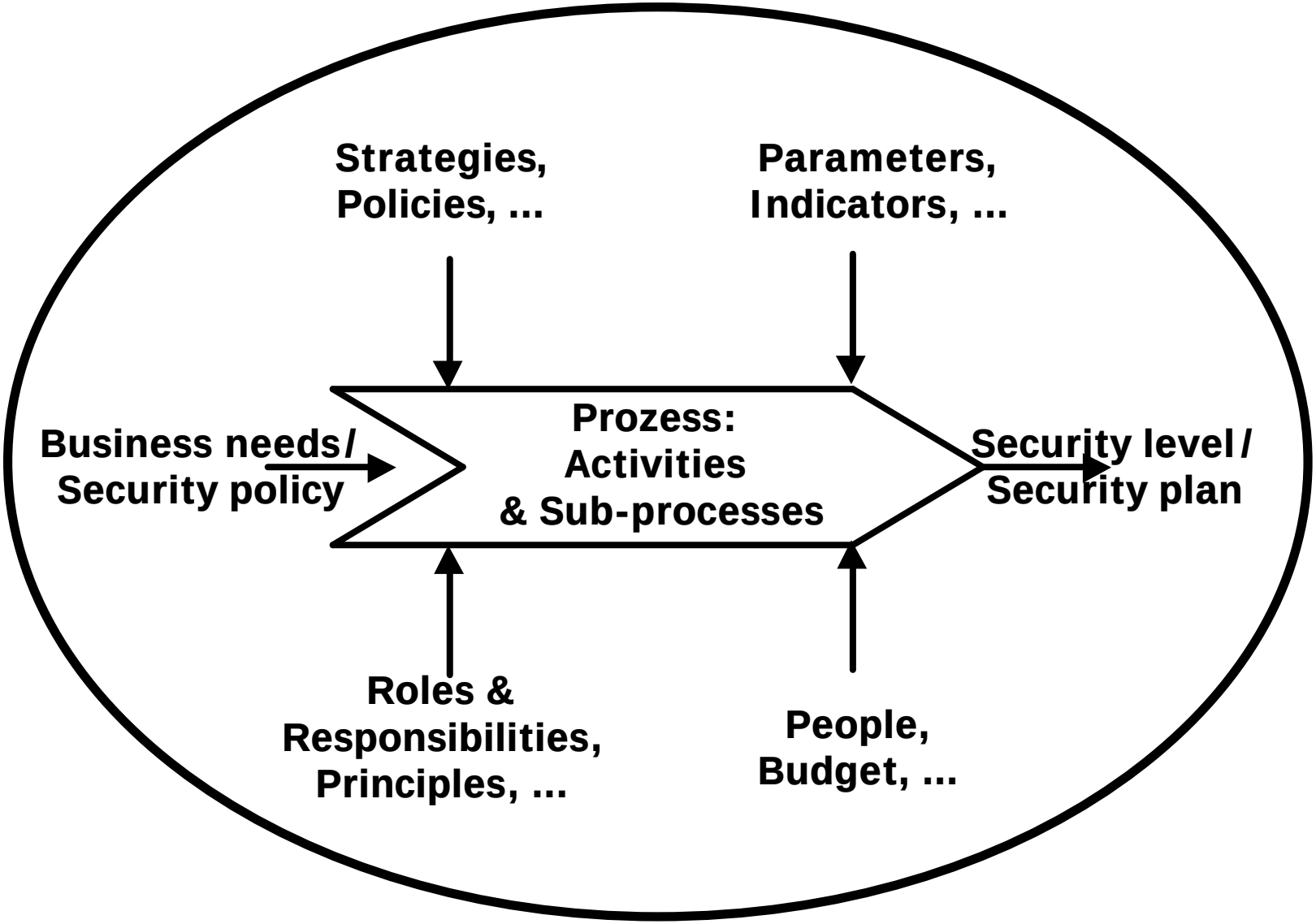
➔ eines ***angemessenen Sicherheitszustands***

⇨ basierend auf einer entsprechenden Aufbau- und Ablauforganisation

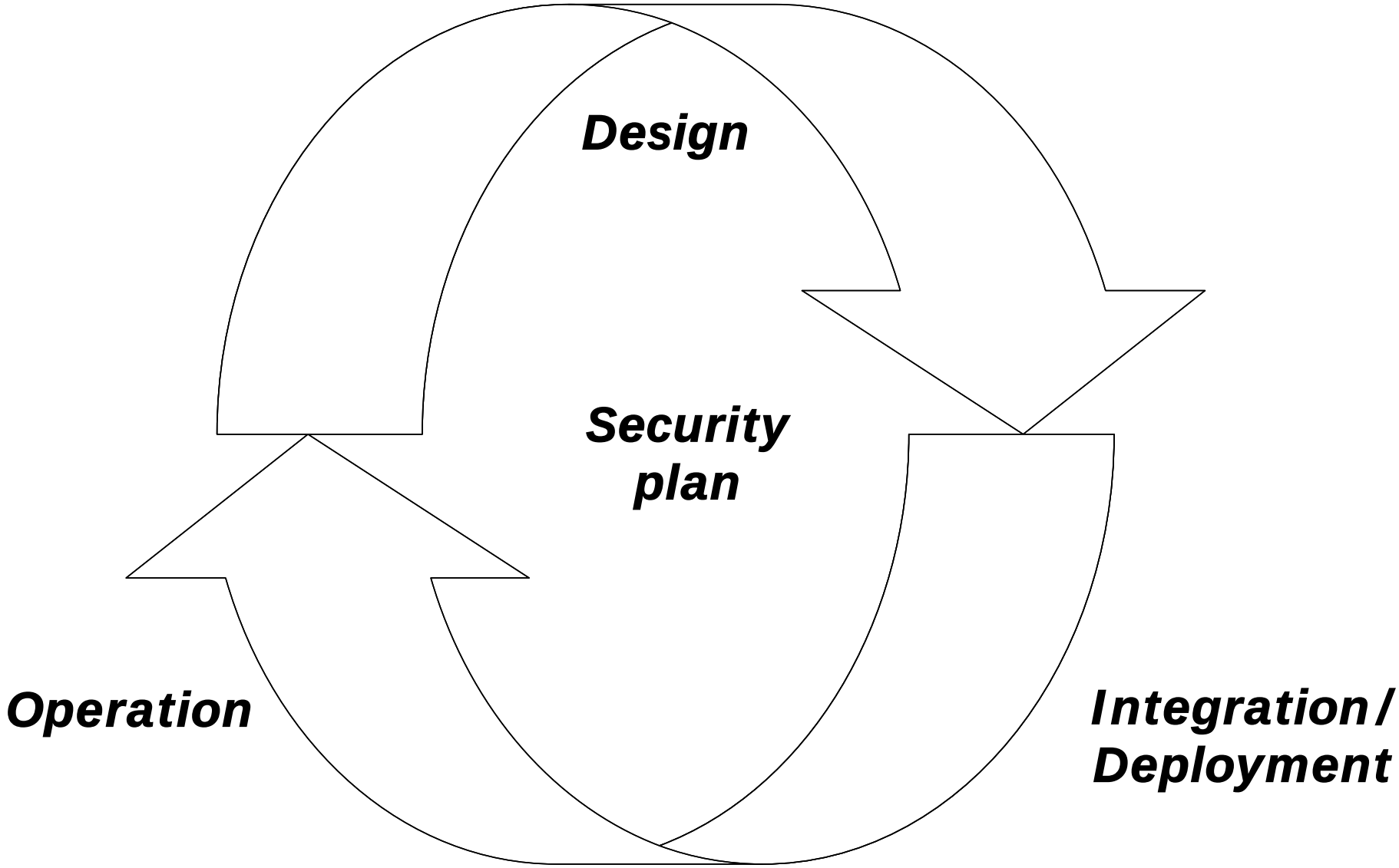
⇨ bezogen auf die Bedürfnisse einer Organisation

- unter Mitwirkung aller Mitglieder
- mittels bestimmter Mittel und Verfahren
- ausgerichtet auf Kunden-/ Mitarbeiterzufriendenheit, langfristigen Geschäftserfolg sowie gesellschaftlichen Nutzen.

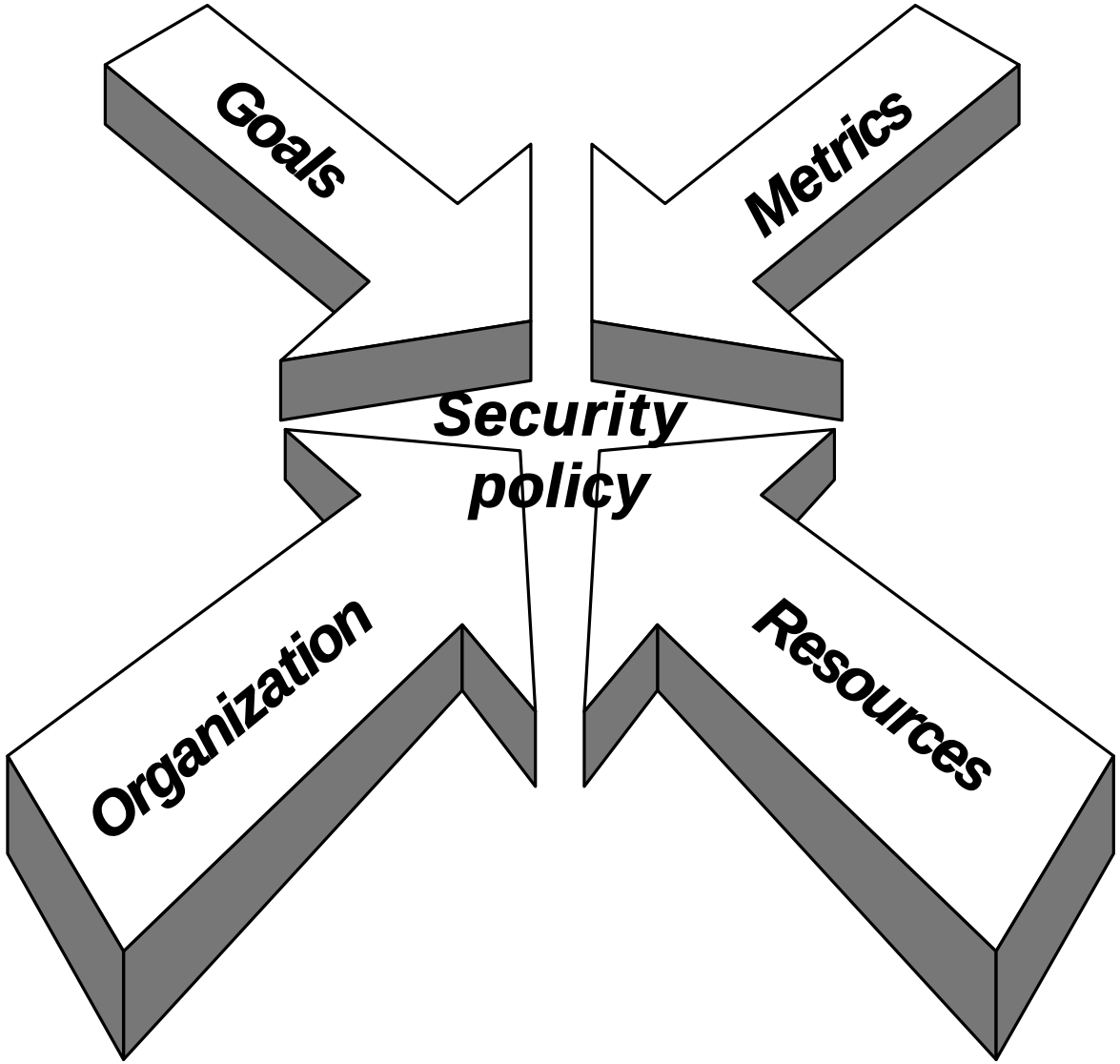
... from the view of a process approach



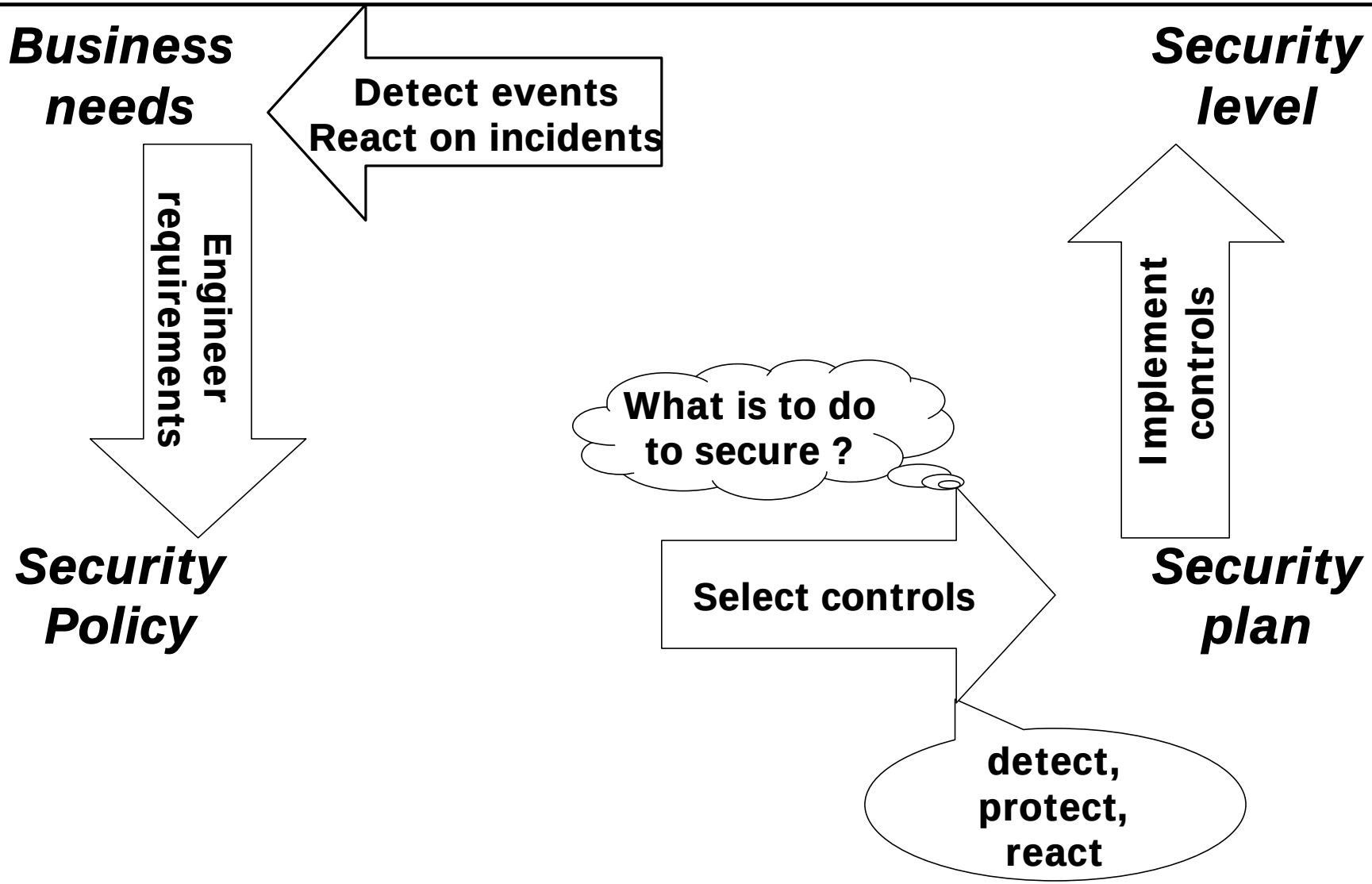
Security management process



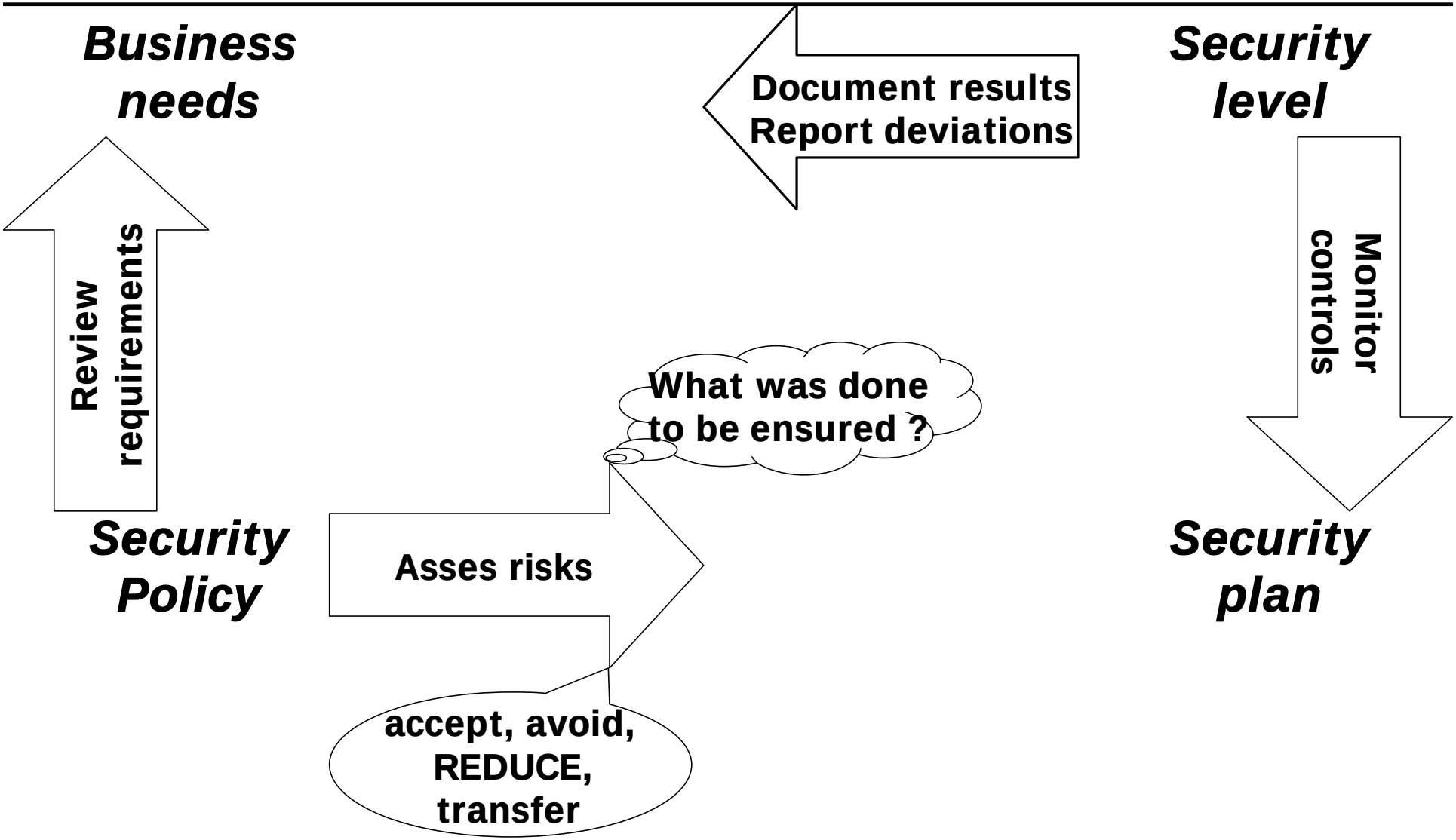
Security management system



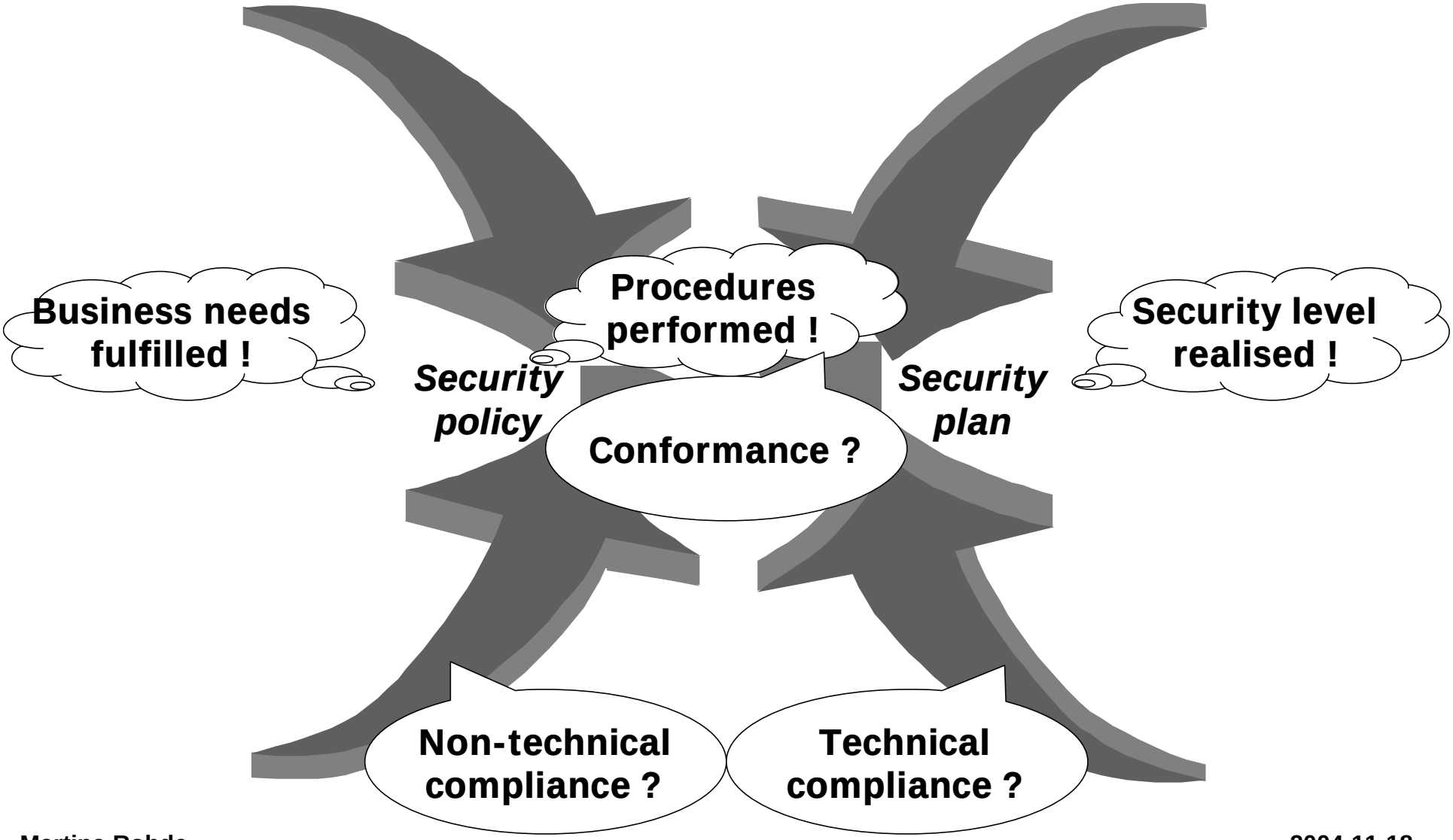
Functionality



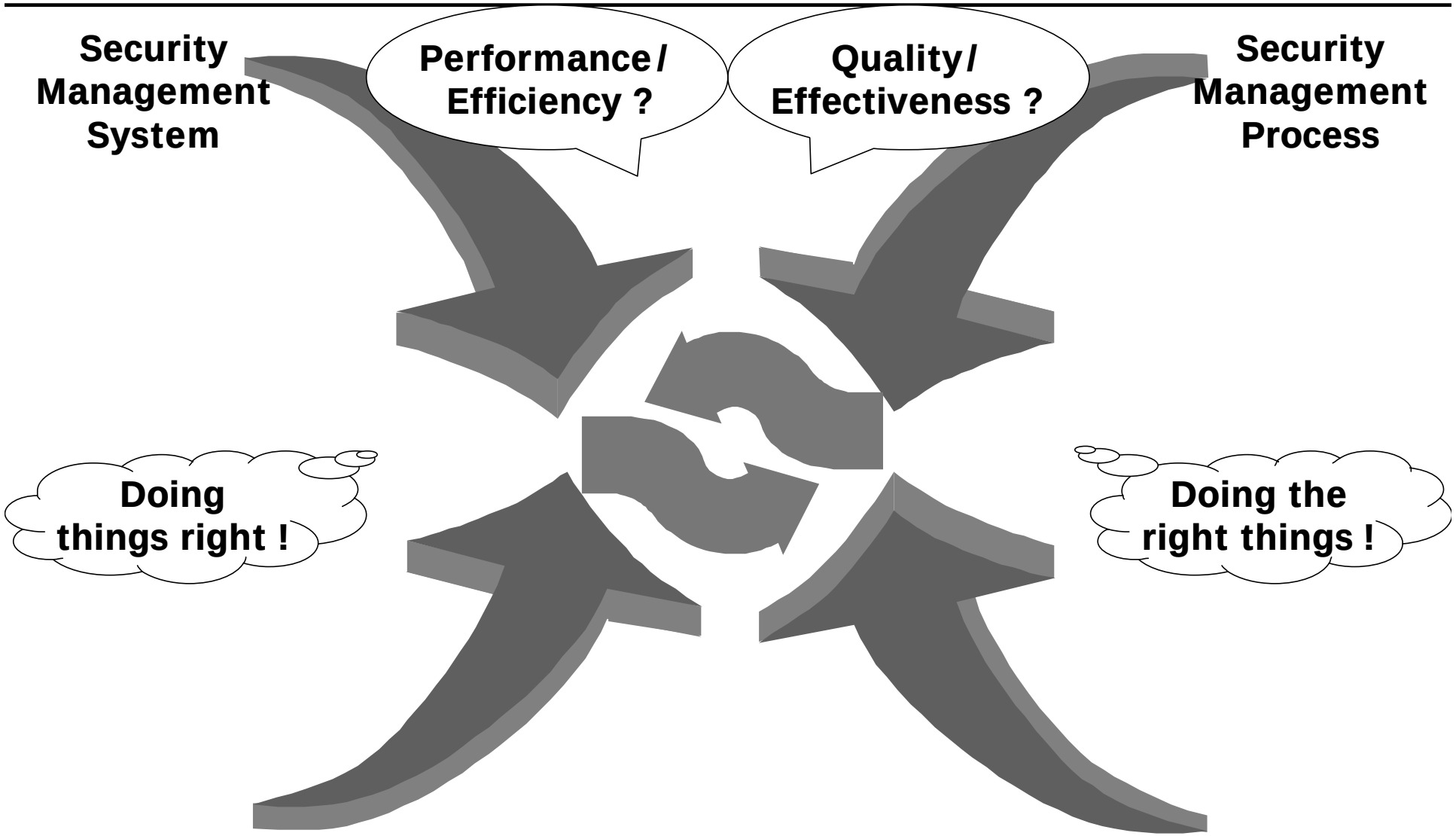
Assurance


Business needs
Document results
Report deviations
Security level
Review requirements
Monitor controls
What was done to be ensured ?
Security Policy
Asses risks
Security plan
accept, avoid, REDUCE, transfer

Assessing Security



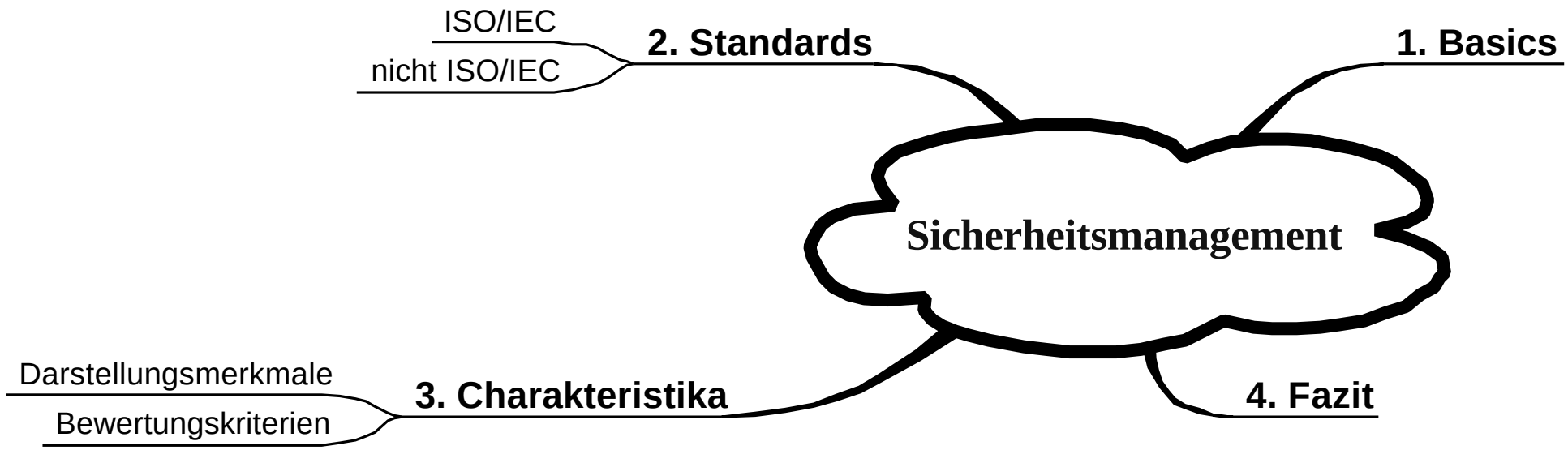
Assessing Security (cont.)



Bundesamt
für Sicherheit in der
Informationstechnik

White box comparison - summary

	purpose	focus	statement	
IS 17799	Process / System	Functionality	Conformance	
IS 13335	System / Process	Functionality / Assurance	Conformance	
BS 7799-2	System	Assurance	Conformance	
BSI IT-BPM	Process / System	Functionality / Assurance	Conformance / Compliance	

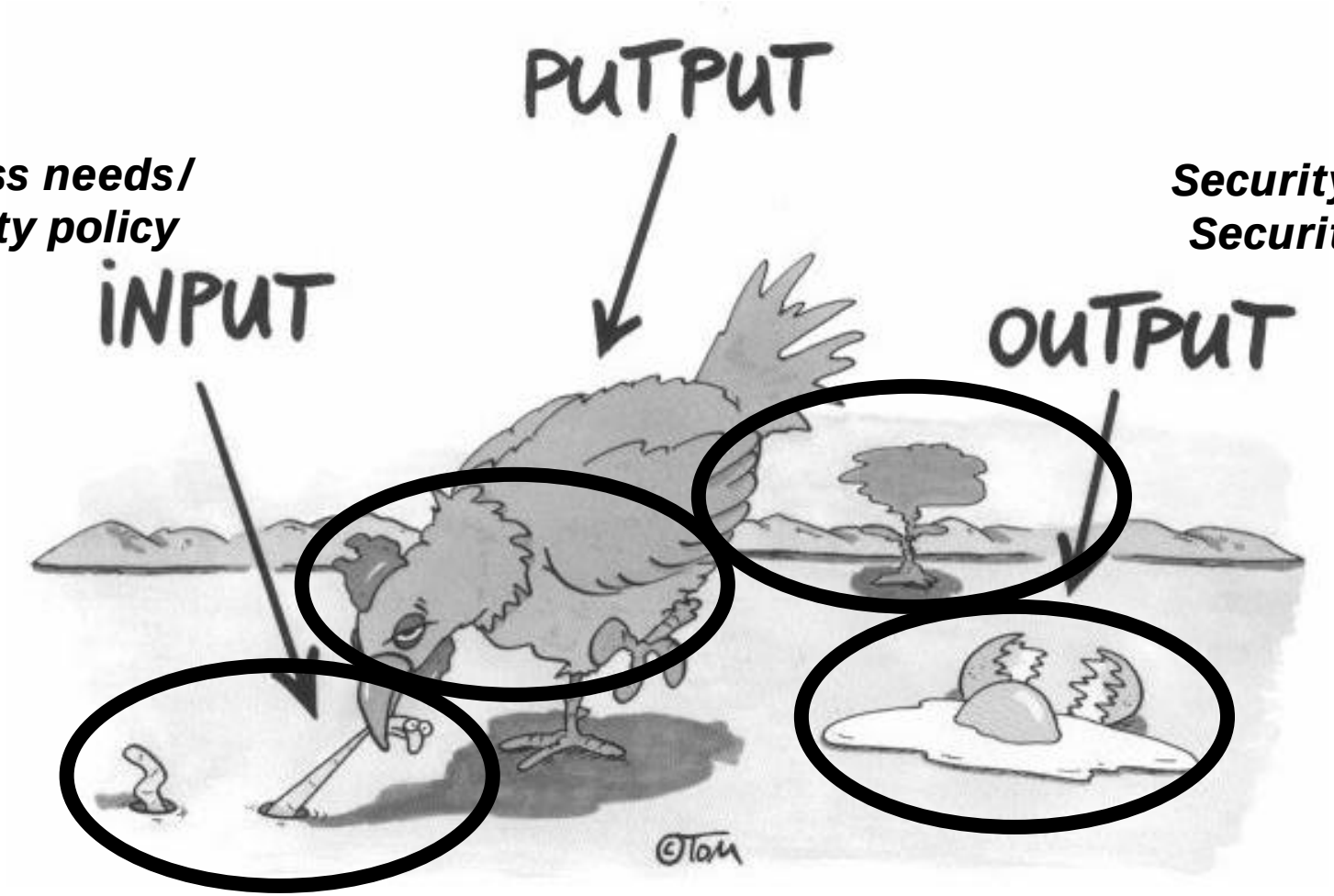

ISO/IEC
nicht ISO/IEC
2. Standards
1. Basics
Sicherheitsmanagement
Darstellungsmerkmale
Bewertungskriterien
3. Charakteristika
4. Fazit

Intro

Process(es) ***Environment***

Business needs/
Security policy

Security level/
Security plan



Vielen Dank für Ihre Aufmerksamkeit !

?

?

?

?

?

?

Fragen ?