Security Frameworks Galore

Thomas Bleier

t@b-sec.net

☎ +43 664 3400559

Classification:	PUBLIC
Version:	01
Date:	11.10.2018
Status:	Final

B-SEC

better secure

https://www.b-sec.net

About me…

- **Thomas Bleier – t@-bsec.net – +436643400559**
- **B-SEC better secure KG**
  - IT-Sicherheit in industriellen Umgebungen (OT / IACS / SCADA, etc.)
  - Assessment – Prüfung techn. und org. Sicherheitsmaßnahmen
  - Training – Security Engineering, Security Architecture, etc.
  - Beratung – Design/Implementierung von sicheren Systeminfrastrukturen
- Security Trainer (Automation Security, Zertifizierungen), FH Lektor
- ISO 27001 Auditor
- Vorsitz OVE AG MR65 Industrial Automation & Control Systems Security
  - MR65 - Spiegelkomittee der IEC TC65 – ISO 62443, ISO 61508, etc.
- Hobbys: u.a. Security Zertifizierungen ☺
  - CISSP, ISSAP, ISSMP, CSSLP, CISA, CISM, GICSP, CEH, IEC62443, SCRUM, ITIL, uvm.

Why do I need a security framework?

- When…
  - … developing technology/devices/systems
  - … operating technology/devices/systems
- Security is **not the only concern** in organizations ☺
  - In fact it‘s one of the least very often… ☹
- Simple, effective solutions to implement an **adequate** level of security are needed…
- Needs and requirements in Organizations are **not that different** at higher abstraction levels
- → that‘s where Security Frameworks come into play

What is a Security Framework?

Standardized Methodology

- Don't invent everything new

Guidance for the process

- How to achieve a desired target state

Set of Tools

- Common vocabulary, best practices

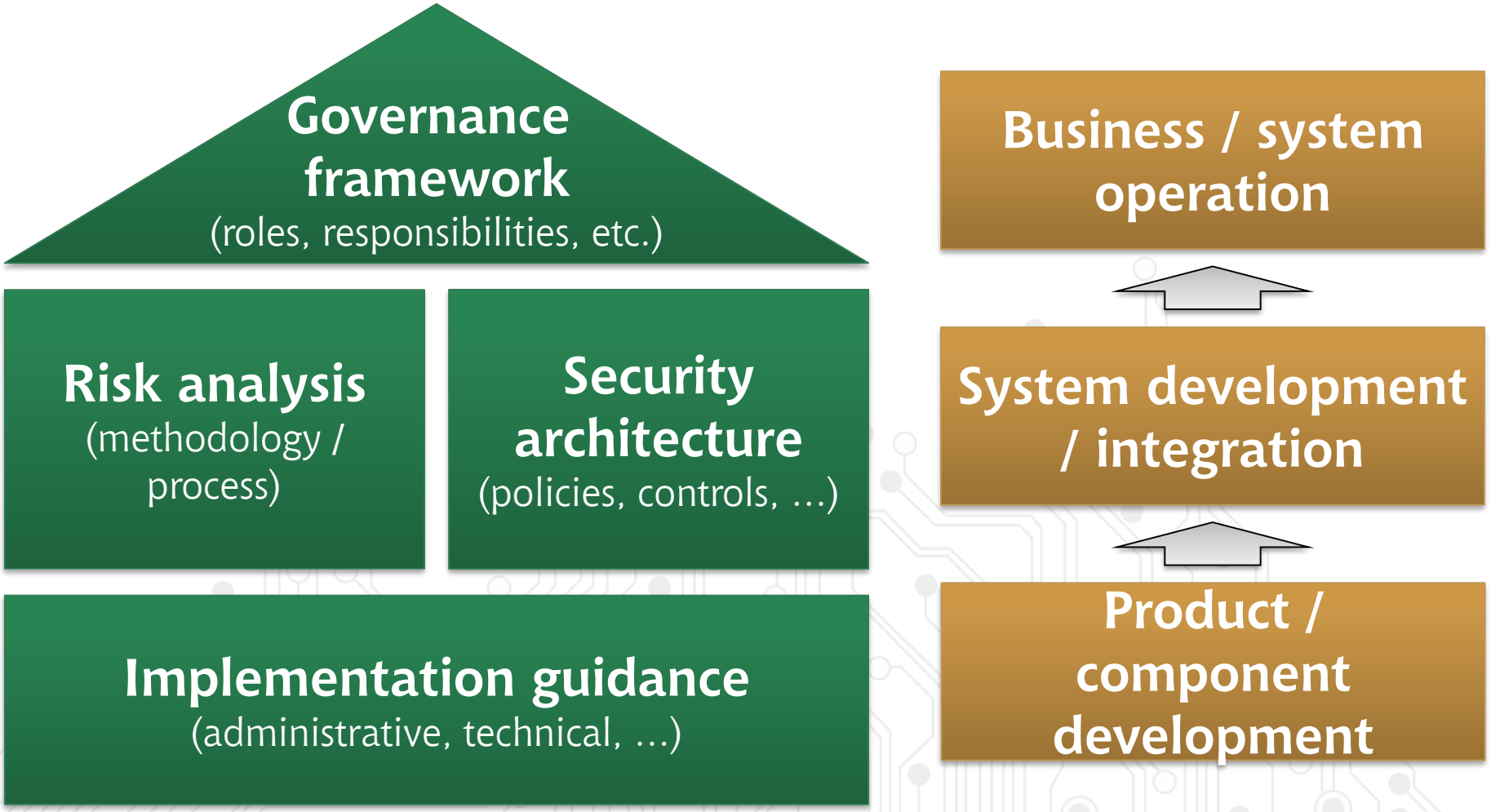
Measurement of the result

- Compliance metrics, audit criteria

Security Aspects

- Confidentiality
- Integrity
- Availability
- Safety
- Reliability
- Resilience
- Privacy
- …

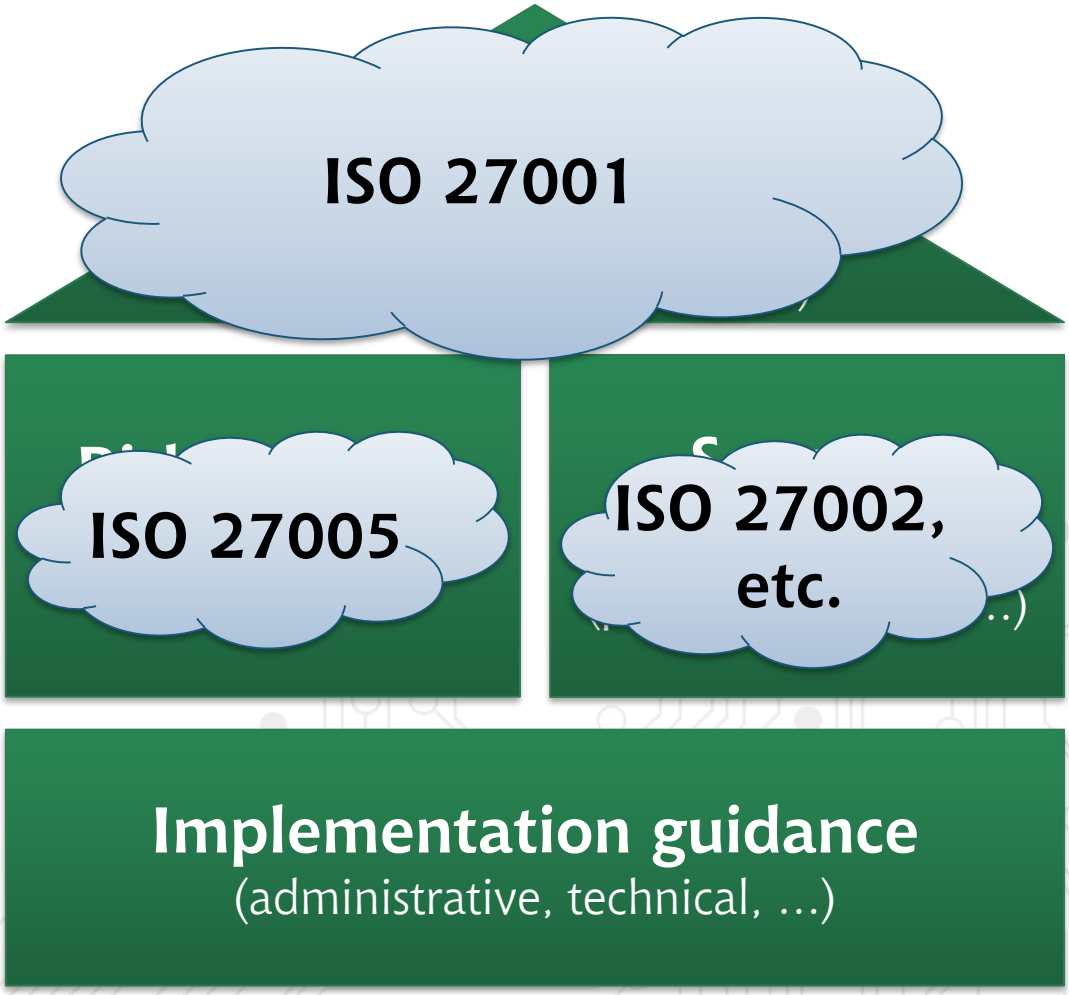
Topics covered by Security Frameworks

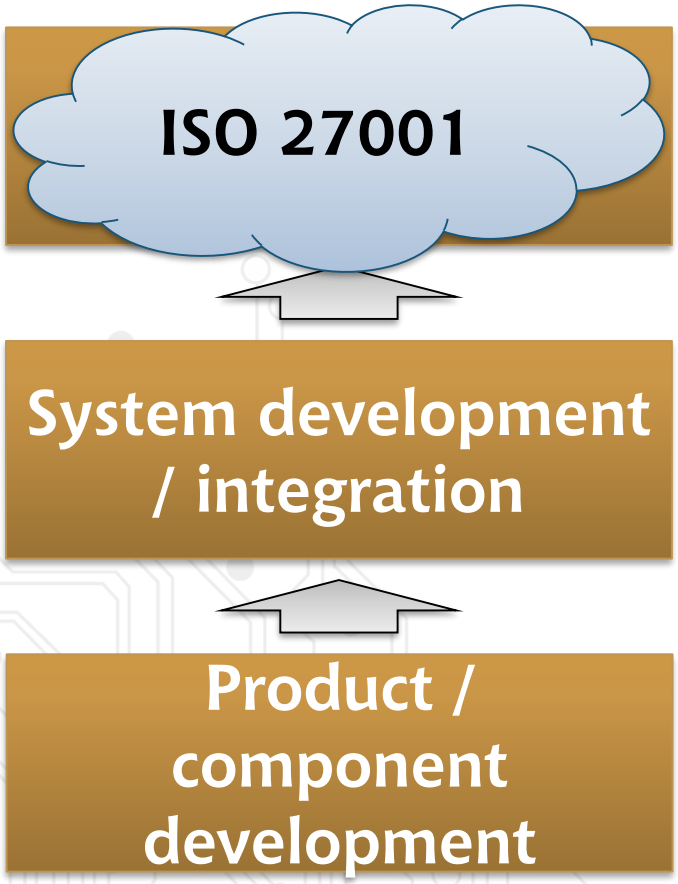


ISO 2700x - Overview

- "State of the Art" for Information Security Management
- Based on a **Management system** (ISO Annex-SL)
- Lot's of standards for specific aspects (182 pub./69 dev.)
- **Certifiable**: ISO 27001 – plus Ext. acc. 27009 (27018/27019/etc.)
- Basic approach
  - Define the ISMS – Scope, Context, Management, Support
  - Analyse the risk – SoA, Objectives, Risk Register
  - Implement controls (Annex A / ISO 27002 plus Extensions)
  - Rinse and repeat ("Monitoring, Evaluation, Improvement")

ISO 2700x - Characteristics

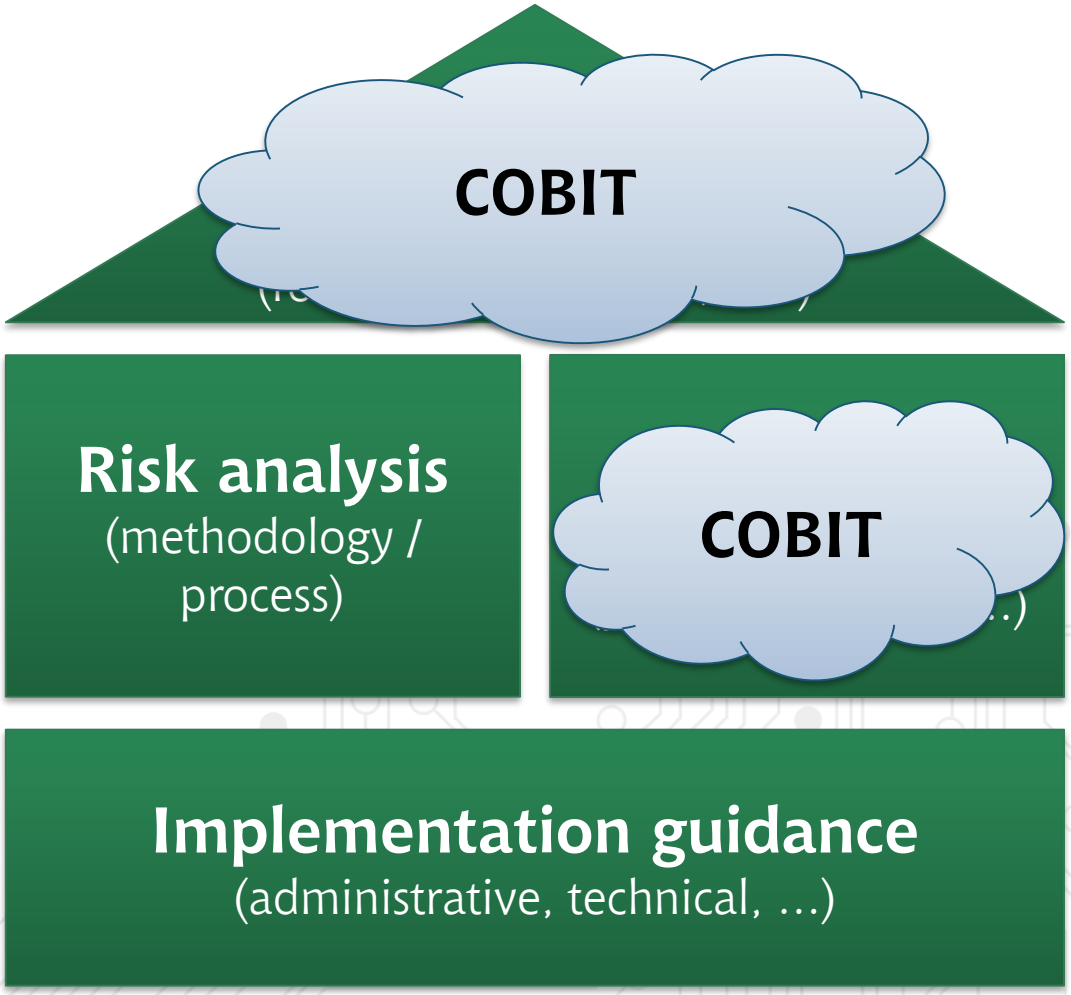


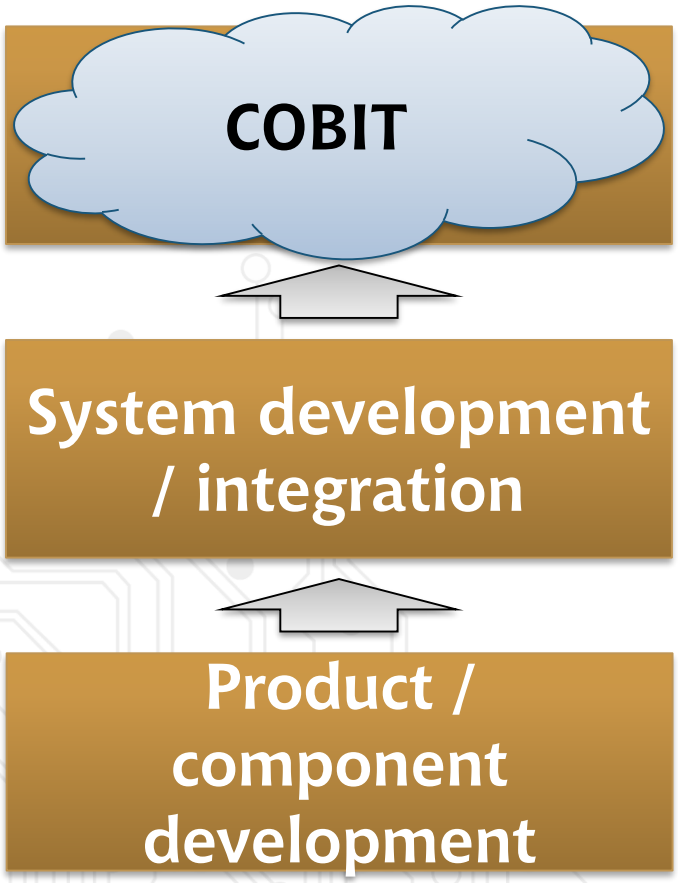


COBIT - Overview

- Previously called "**Control Objectives for Information and Related Technology**"
- **Governance**-based approach to design of corporate IT
- Align IT architecture and operations to **Business Goals**
- Measure effectiveness and improve
- Control objectives mapped to 37 IT processes / 5 domains
- **COBIT 5 for Information Security** – adoption of COBIT approach to information security

COBIT - Characteristics

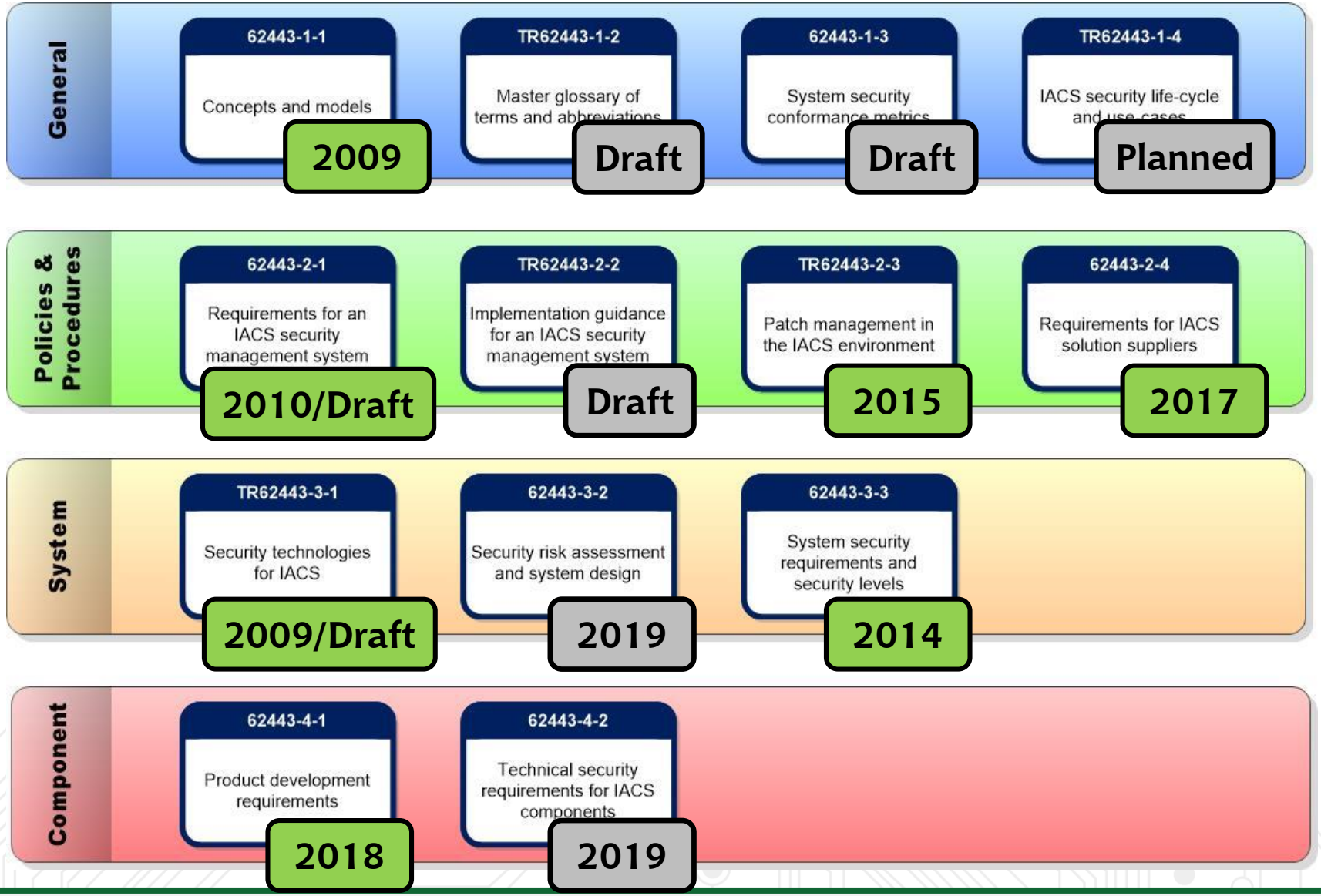




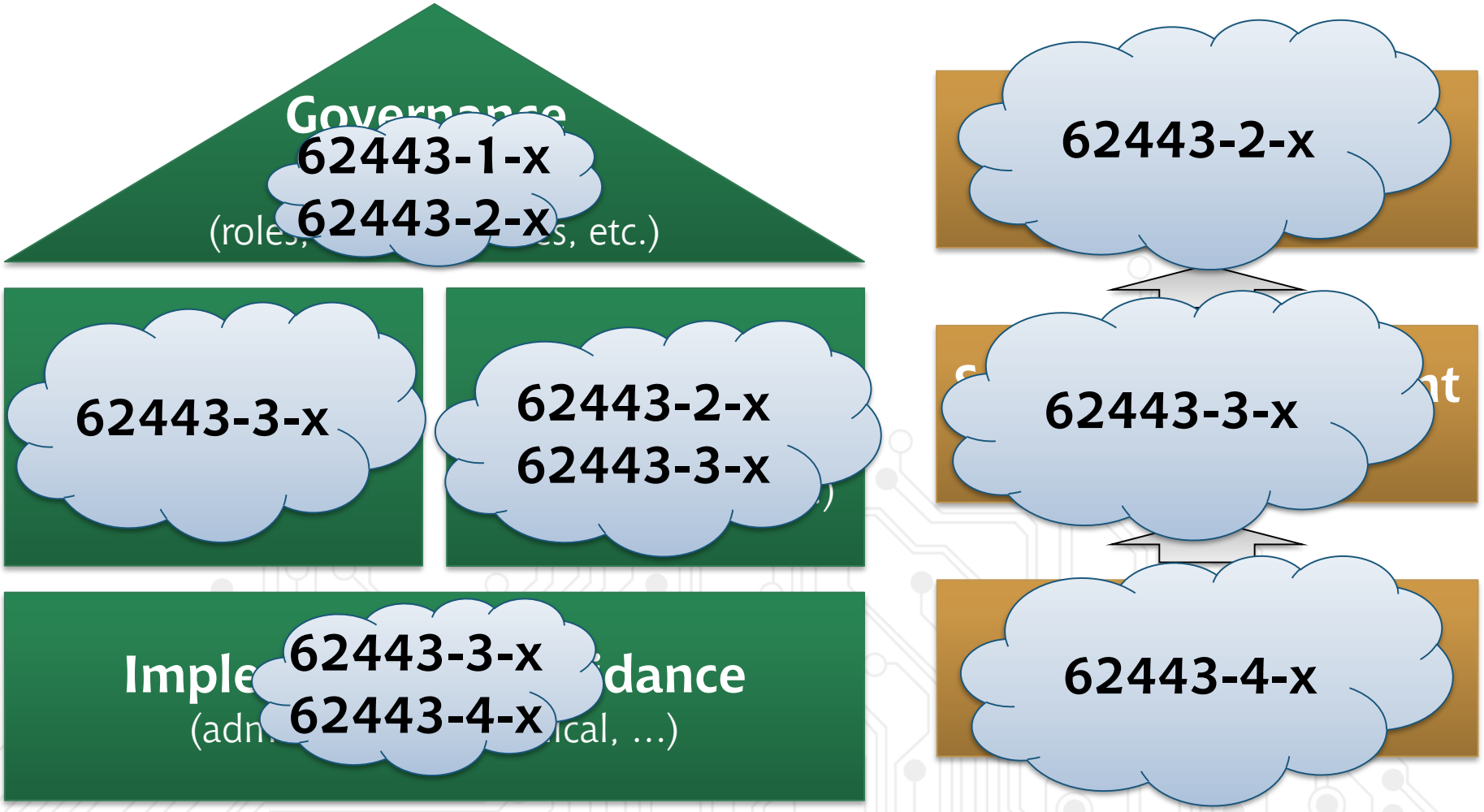
IEC 62443 - Overview

- Cybersecurity for **Industrial Automation and Control Systems (IACS)**
- 13 Standards under development
- Differentiates between **Supplier – Integrator – Operator**
- Specific standards for Component Development / System Development / System Operation/Management
- **Risk-based approach** (Threat and Risk assessment)
- **Security Levels** based on est. **attacker capability**
- Only partly finished, a number of topics not yet addressed

IEC 62443 - Overview

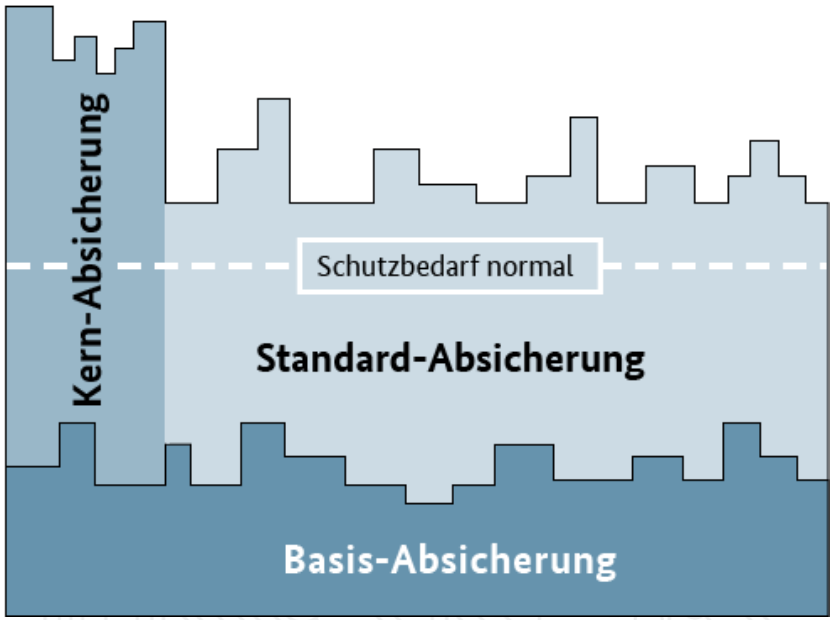


IEC 62443 - Characteristics

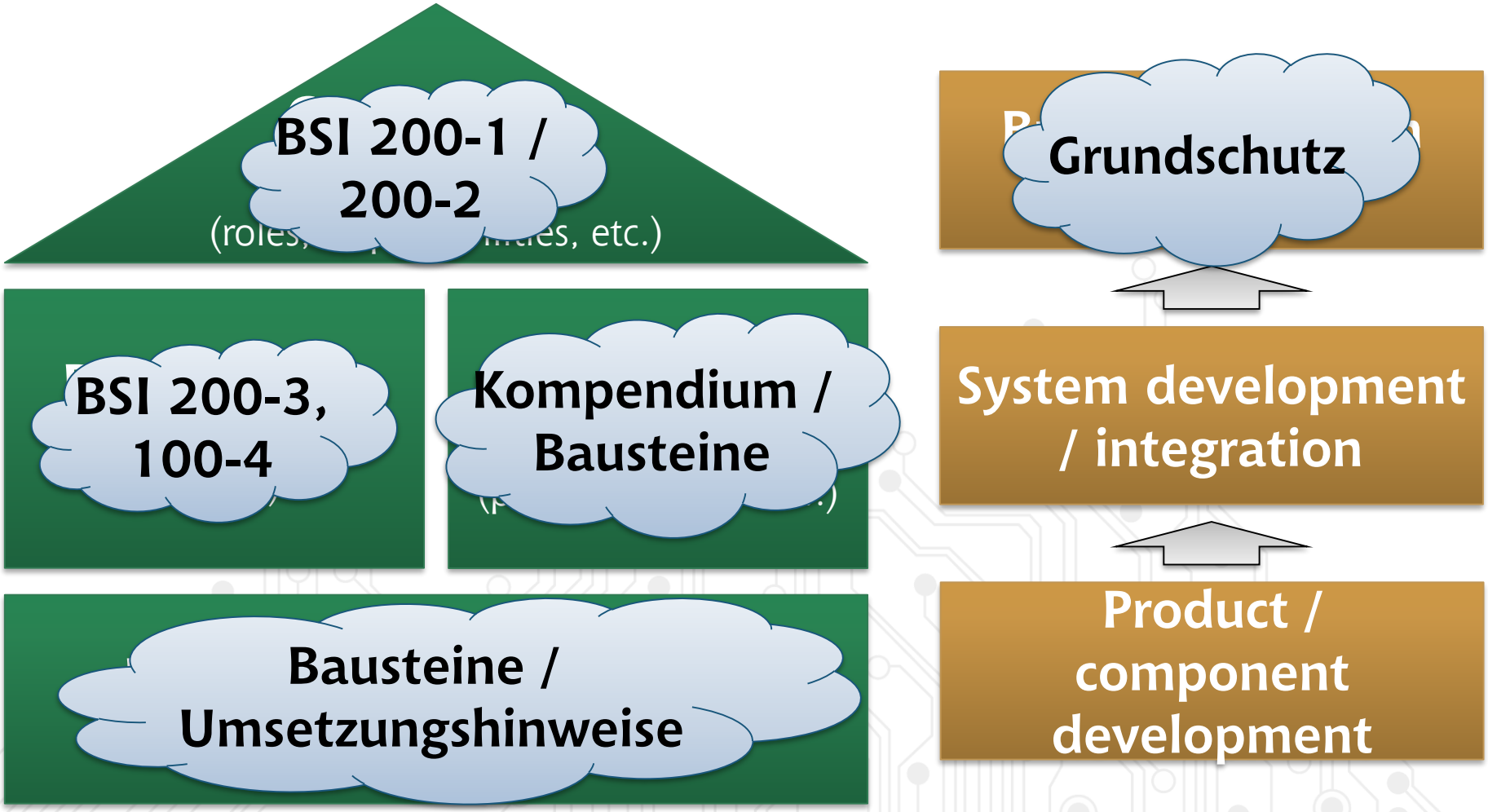


BSI Grundschutz - Overview

- **2018 - New edition** – 200-x Standards, Kompendium
- Risk analysis based on 47 basic threats
- Differentiates **base- / core- / standard protection**
- Very **extensive and detailed set of controls**/measures
- Includes standard for BCM / BIA (100-4)
- Freely available



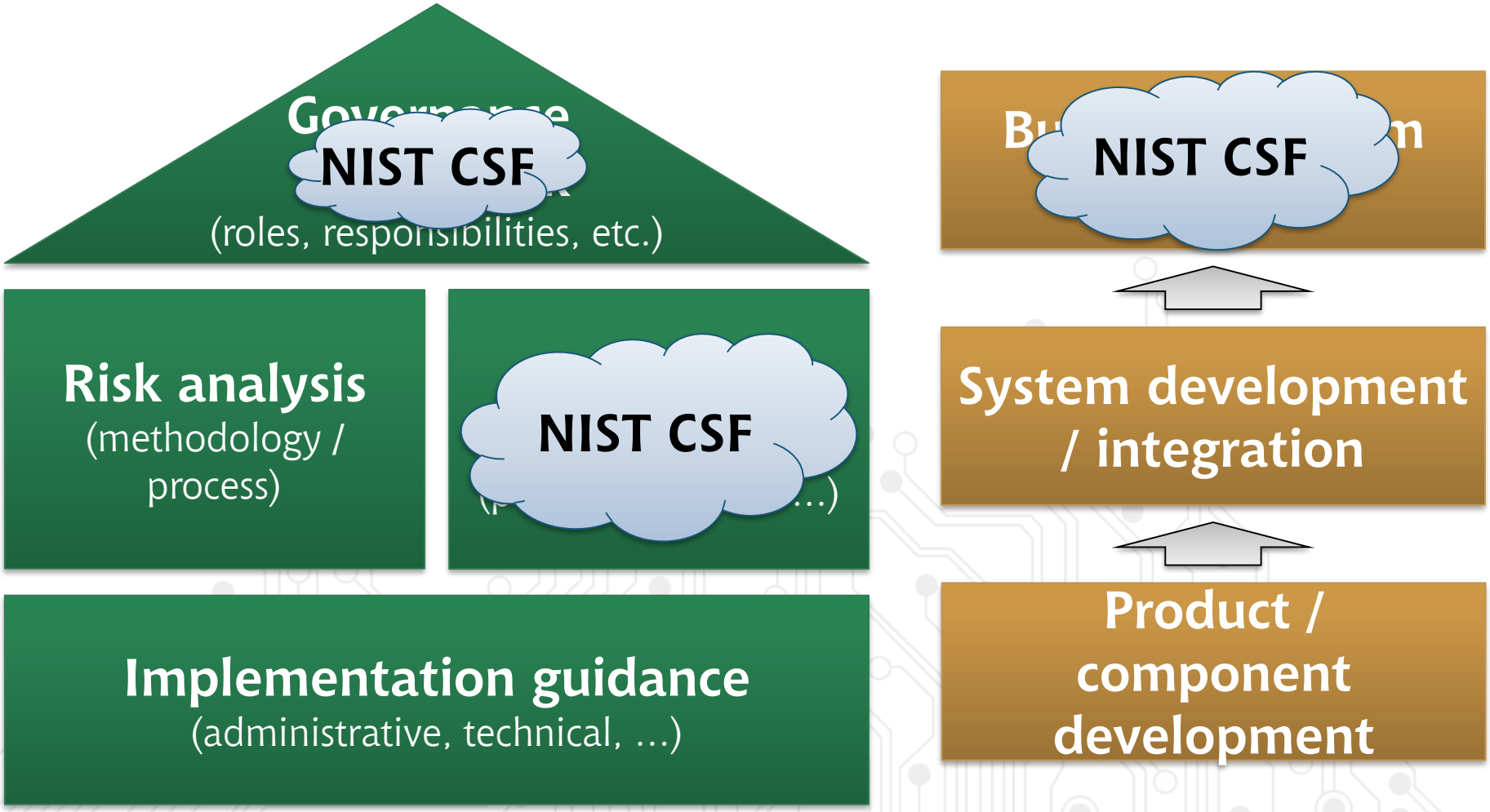
BSI Grundschutz - Characteristics



NIST Cybersecurity Framework - Overview

- Lightweight framework for improving critical infrastructure cybersecurity – "smooth" start into topic
- **4 implementation tiers** – "sophistication level"
- "Simple" approach based on **5 functions**
- 108 controls in 23 categories, aligned to those 4 functions
- **Detect – Respond – Recover**
- **Mapped/aligned** with ISO 27001, COBIT, CIS CSC, IEC 62443, NIST SP800-53

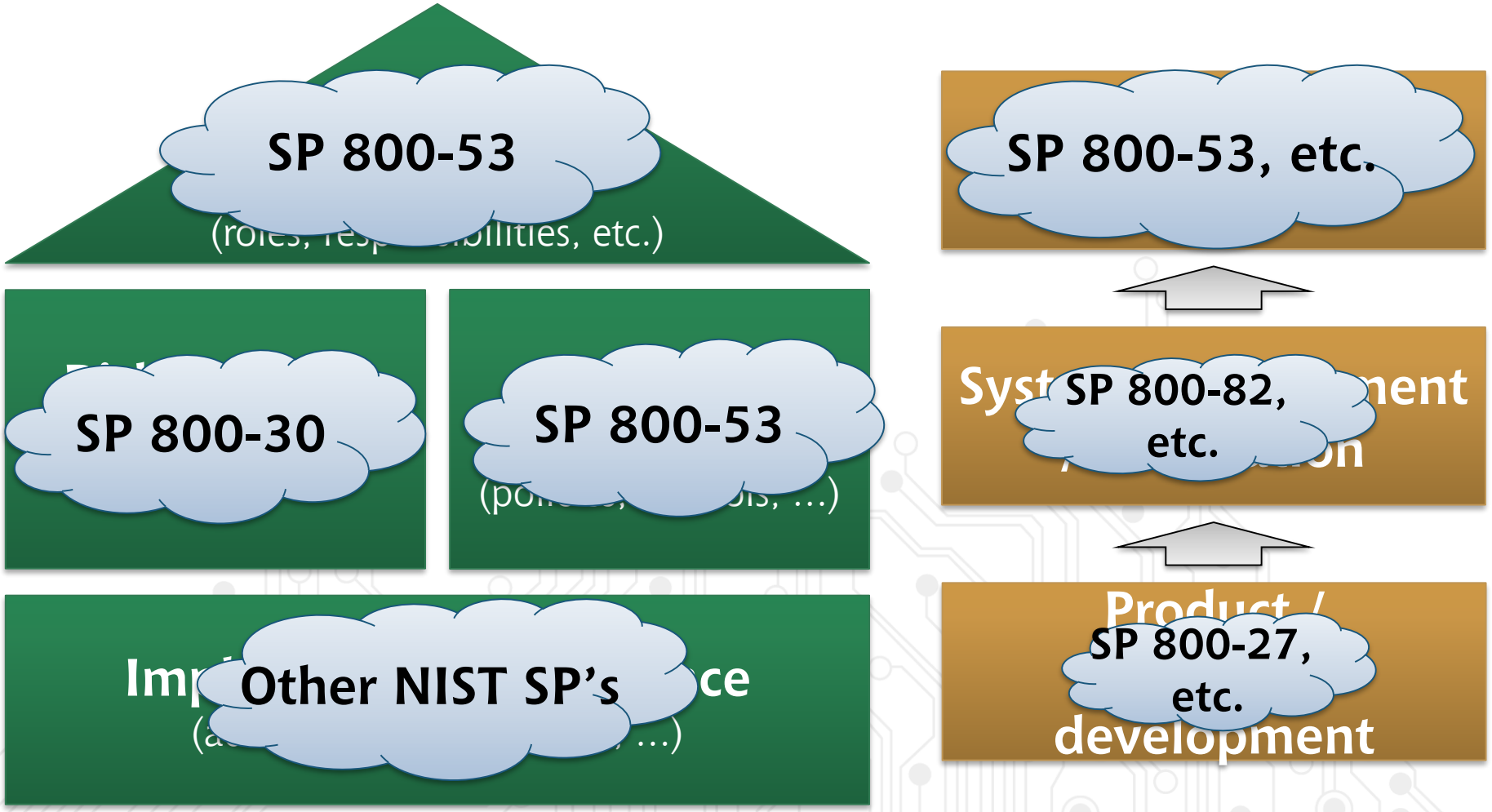
NIST Cybersecurity Framework - Characteristics



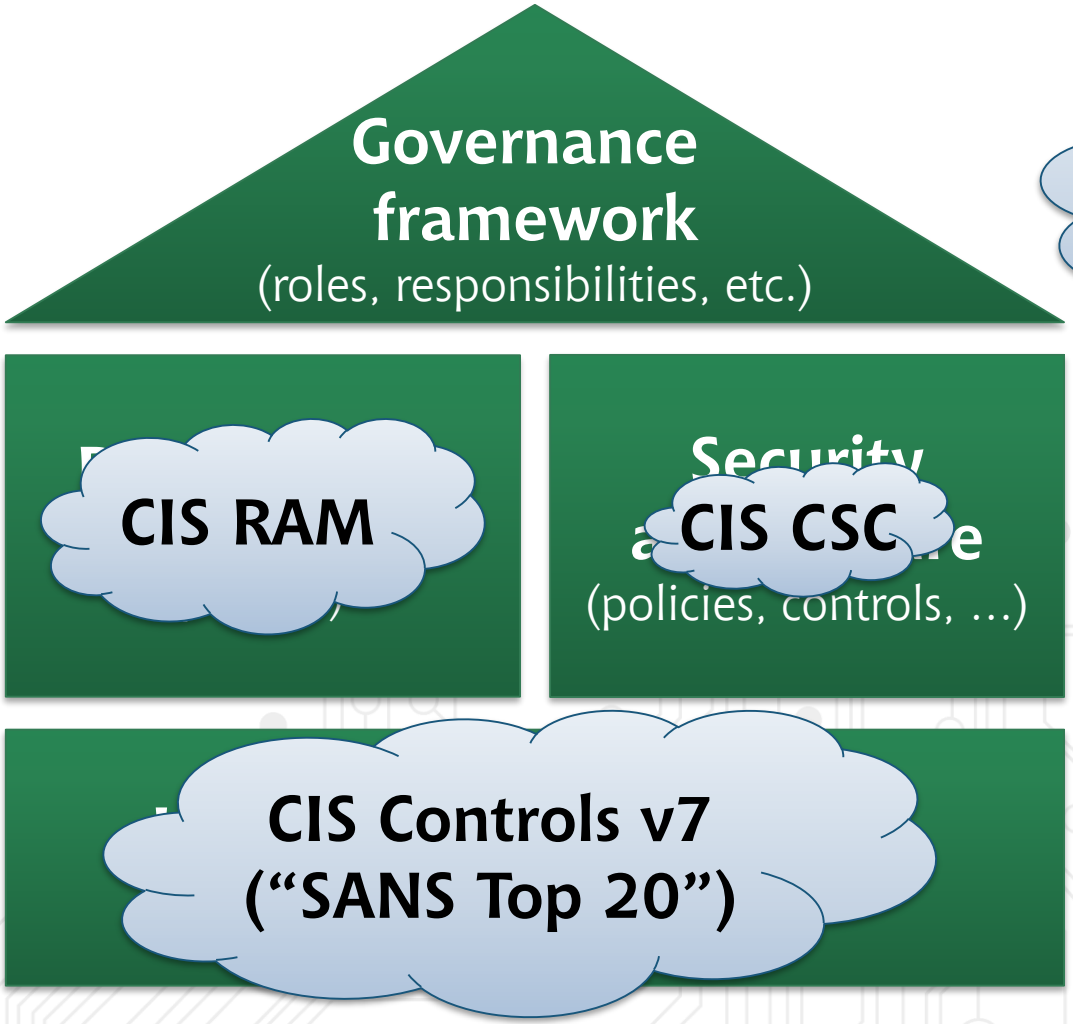
NIST SP 800-53 etc. - Overview

- US National Institute of Standards & Technology – US Gov.
  NIST SP 800-53r4 – Security and Privacy Controls for Federal Information Systems and Organizations – and others
- Extensive **control-set** (212 total)
- **Categorization** of Systems based on FIPS 199: low-impact, moderate-impact, high-impact for C-I-A
- "Checklist-based" approach
- Mappings to and from ISO 27001 / ISO 15408

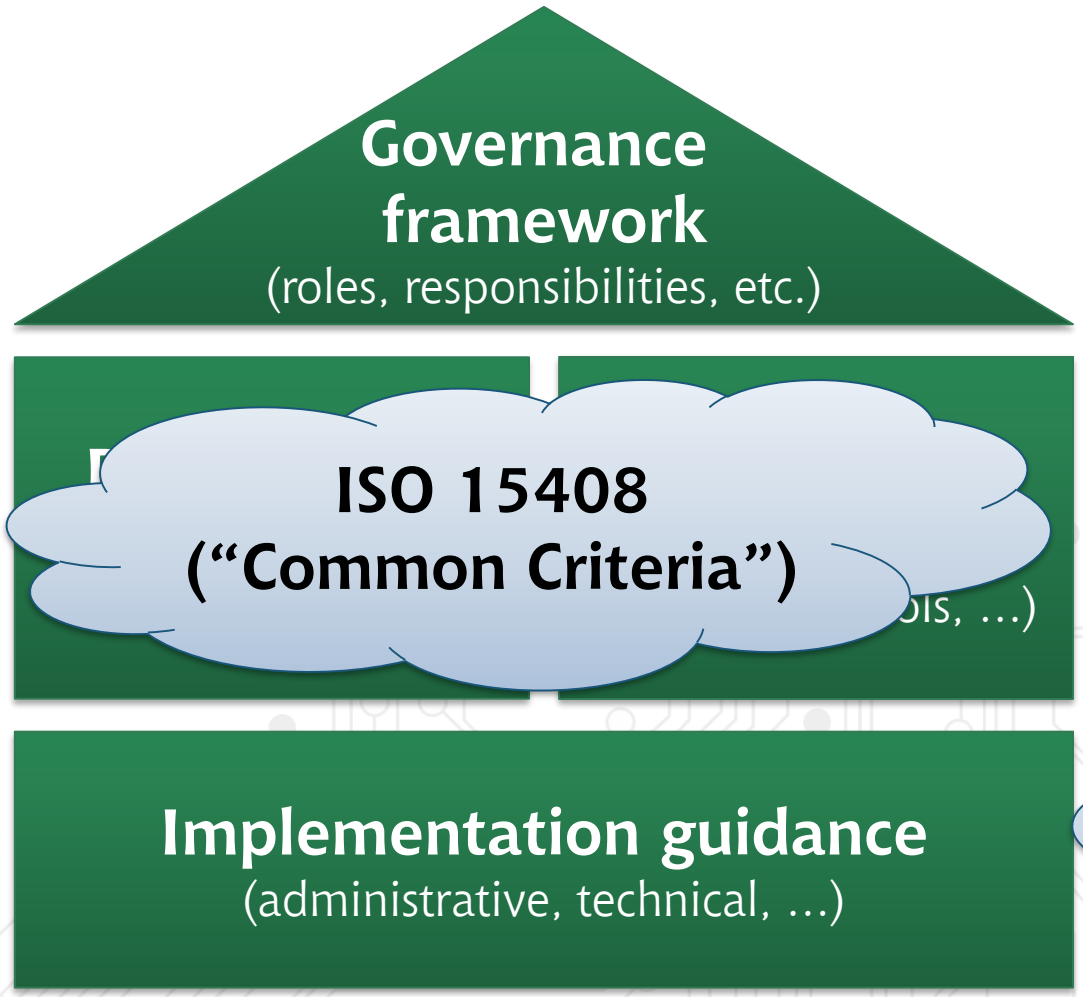
NIST SP 800-53 etc. - Characteristics

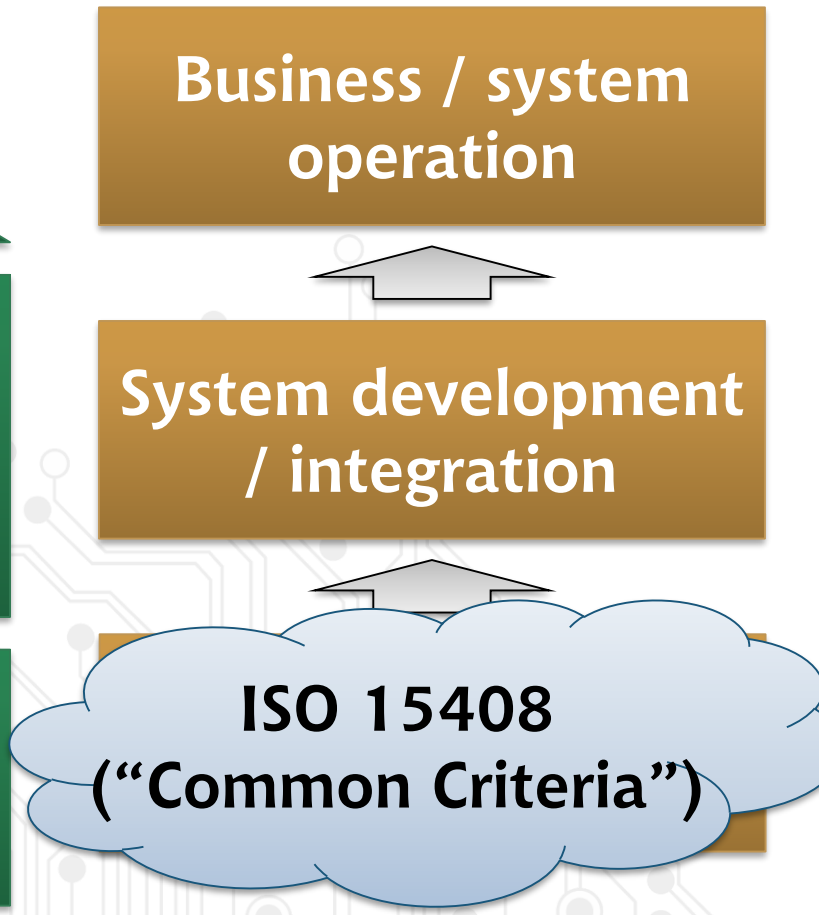


Other Frameworks – CIS Critical Security Controls v7

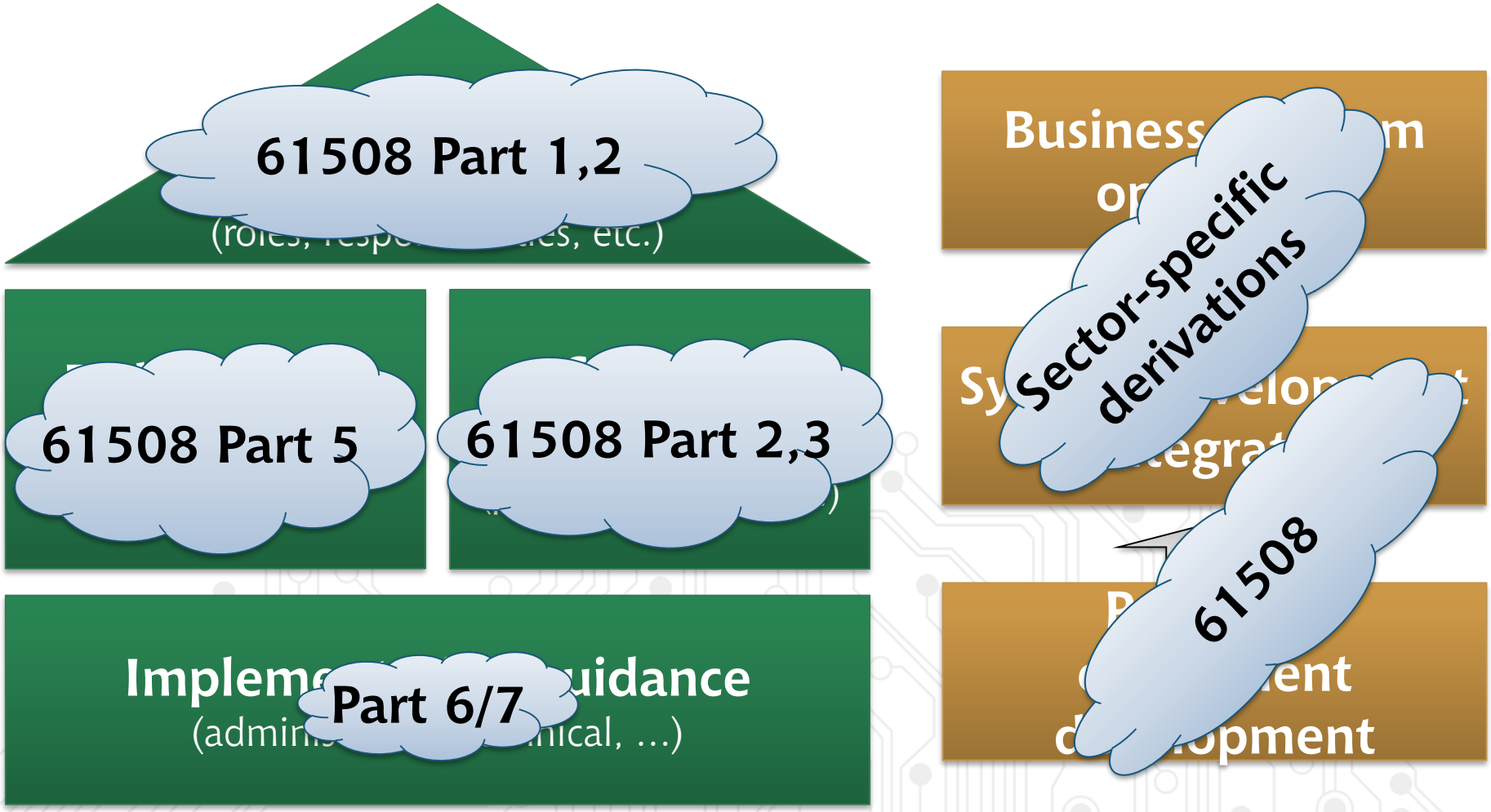


Other Frameworks – ISO 15408 Common Criteria

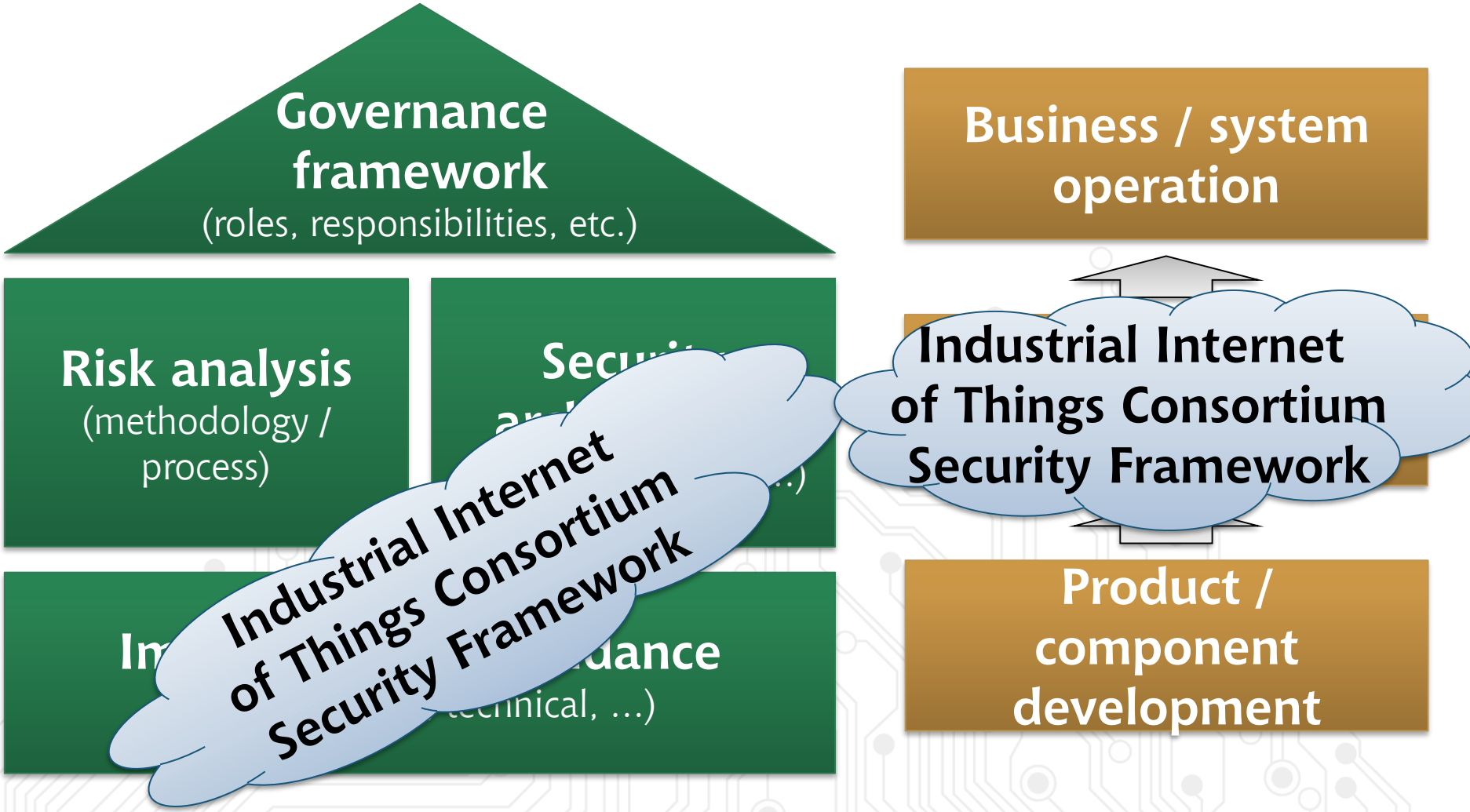




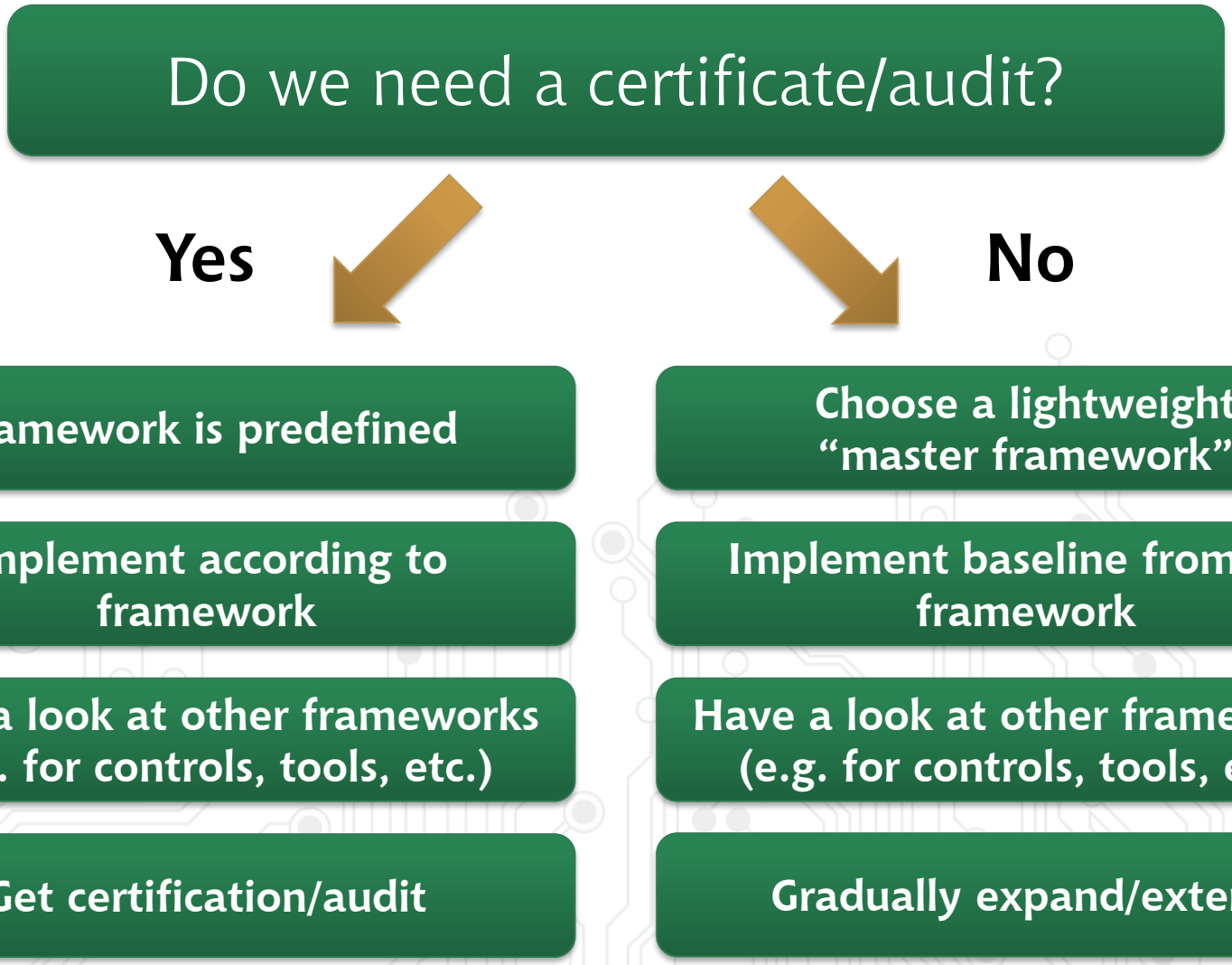
Other Frameworks – IEC 61508 - functional safety



Other Frameworks – Industrial IoT Consortium



Which framework to implement?



Remember

- Security Frameworks are no silver bullet – but they can **facilitate the process** and **reduce the effort** of raising the security level in organizations
- Each framework has strengths and weaknesses – **pick & choose**, they align well (mostly ☺)

Contact

Thomas Bleier

Dipl.-Ing. MSc CISSP-ISSAP,ISSMP CISA CISM CSSLP GICSP CEH

t@b-sec.net ☎ +43 664 3400559

https://www.b-sec.net