Security Testing for Compliance: Meeting Standards, Reducing Risk

DistriNet

A level of Quality or Attainment

Standard

Technology

V

- Road vehicles
- Payment cards
- Embedded systems
- Industrial Control systems
- Information systems
- Digital systems

H

Concern

- Interoperability
- Safety
- Security
- Privacy

Role

- Operators
- Integrators
- Manufacturers

DistriNet

A level of Quality or Attainment

Standard

ISO/TR 4804

ISO/SAE 21434

Common Criteria

IEC 61508

IEC62443

EN 18031

ISO 27001

ETSI EN 303 645

NBN EN 17529:2022

DistriNet

A level of Quality or Attainment

Standard

Technology

Road vehicles

Payment cards

Embedded systems

Industrial Control systems

Information systems

Digital systems

Concern

Interoperability

Safety

Security

Privacy

Role

Operators

Integrators

Manufacturers

DistriNet

A level of Quality or Attainment

ISO 27001

Technology

Road vehicles

Payment cards

Embedded systems

Industrial Control systems

Information systems

Digital systems

Concern

Interoperability

Safety

Security

Privacy

Role

Operators

Integrators

Manufacturers

DistriNet

A level of Quality or Attainment

IEC61508

Technology

Road vehicles

Payment cards

Embedded systems

Industrial Control systems

Information systems

Digital systems

Concern

Interoperability

Safety

Security

Privacy

Role

Operators

Integrators

Manufacturers

DistriNet

A level of Quality or Attainment

IEC62443

Technology

Road vehicles

Payment cards

Embedded systems

Industrial Control systems

Information systems

Digital systems

Concern

Interoperability

Safety

Security

Privacy

Role

Operators

Integrators

Manufacturers

DistriNet

Mandatory Quality or Attainment

A level of Quality or Attainment

legislation

Standard

legislation

Technology

Road vehicles
Payment cards
Embedded systems
Industrial Control systems
Information systems
Digital systems

Concern

Interoperability
Safety
Security
Privacy

Role

Operators
Integrators
Manufacturers

DistriNet

legislation

Technology

Road vehicles

Payment cards

Embedded systems

Industrial Control systems

Information systems

Digital systems

Concern

Interoperability

Safety

Security

Privacy

Role

Operators

Integrators

Manufacturers

DistriNet

legislation

Product requirements

RED-DA
(August 2025)

“make systems cyber secure”
(radio equipment)

Product Requirements + Product Lifecycle

CRA
(December 2027)

“make systems cyber resilient”
(digital systems)

DistriNet

legislation

Standard

Product requirements

RED-DA
(August 2025)

Product Requirements + Product Lifecycle

CRA
(December 2027)

ETSI EN 303 645

IEC62443

Common Criteria

EN 18031

requirements

requirements + lifecycle

requirements + lifecycle

requirements

DistriNet

- Authentication & access control
- Data protection
- No known vulnerabilities
- logging
- Secure updates
- Mitigate DoS attacks
- Control attack (surface)
- intervenience
- Network monitoring
- transparency

RED-DA
(August 2025)

Requirement	3.3.(d)	3.3.(e)	3.3.(f)
[ACM] Access control mechanism	✓	✓	✓
[AUM] Authentication mechanism	✓	✓	✓
[SUM] Secure update mechanism	✓	✓	✓
[SSM] Secure storage mechanism	✓	✓	✓
[SCM] Secure communication mechanism	✓	✓	✓
[LGM] Logging mechanism	-	✓	✓
[DLM] Deletion mechanism	-	✓	-
[UNM] User notificiation mechanism	-	✓	-
[RLM] Resilience mechanism	✓	-	-
[NMM] Network monitoring mechanism	✓	-	-
[TCM] Traffic control mechanism	✓	-	-
[CCK] Confidential cryptographic keys	✓	✓	✓
[GEC] General equipment capabilities	✓	✓	✓
[CRY] Cryptography	✓	✓	✓

EN 18031

DistriNet

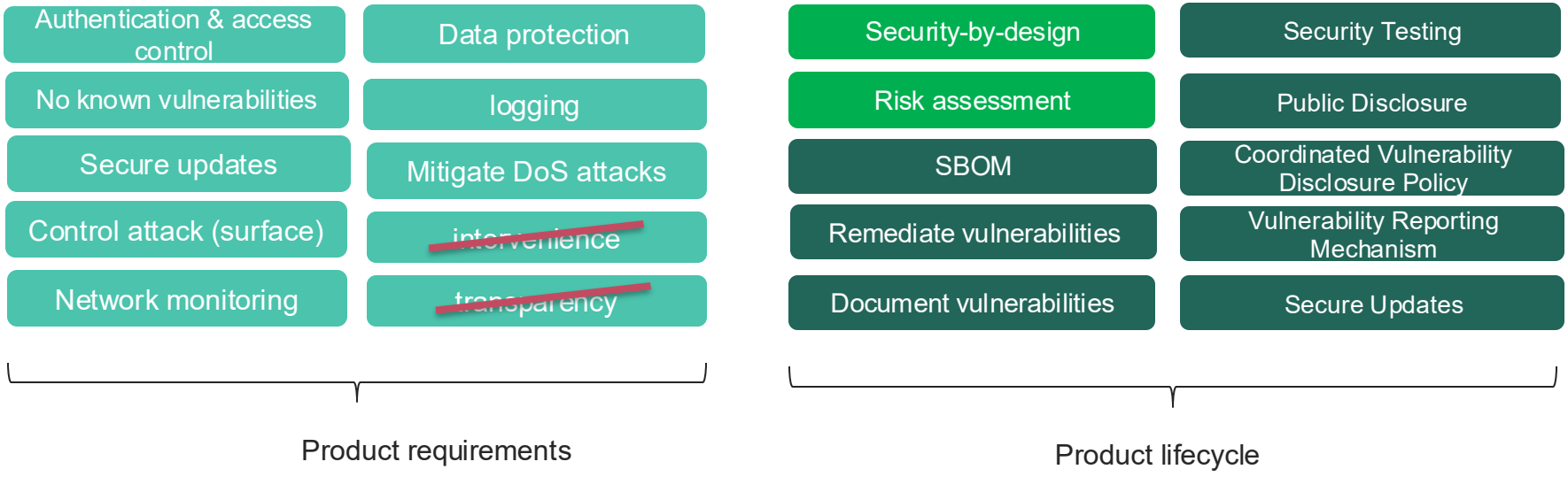
legislation

RED-DA
(August 2025)

“make systems cyber secure”

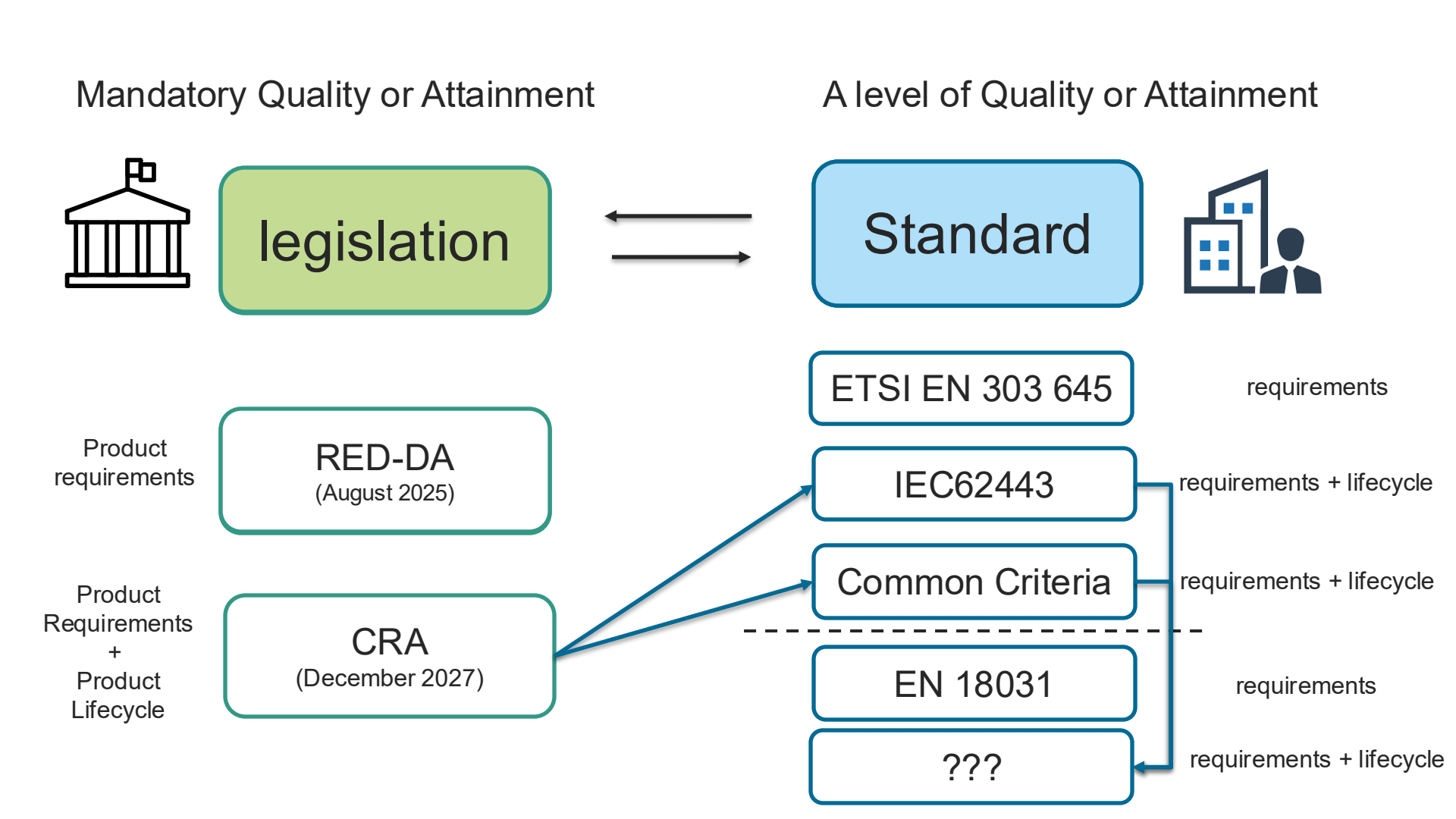
CRA
(December 2027)

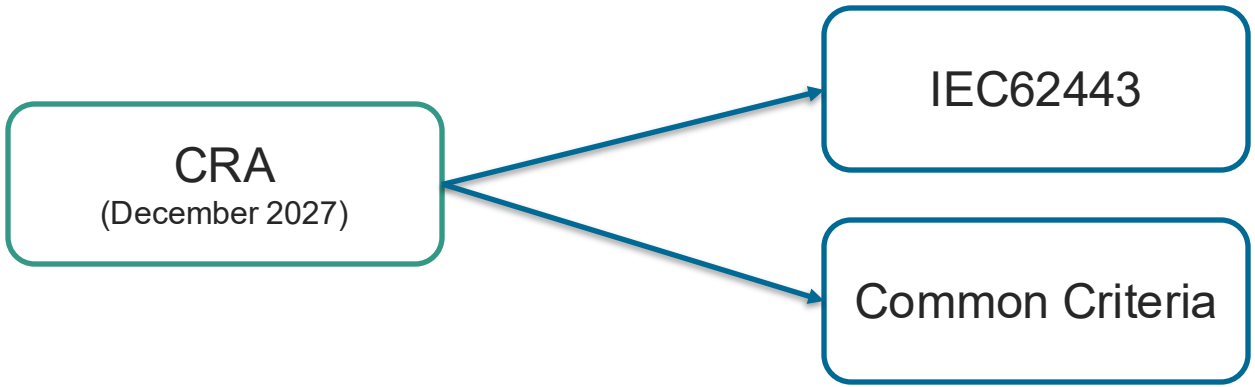
“make systems cyber resilient”

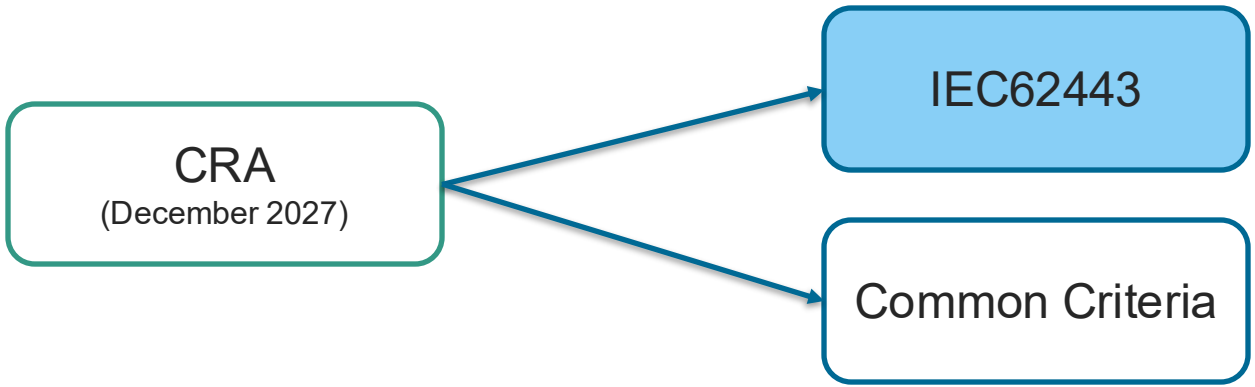


CRA
(December 2027)

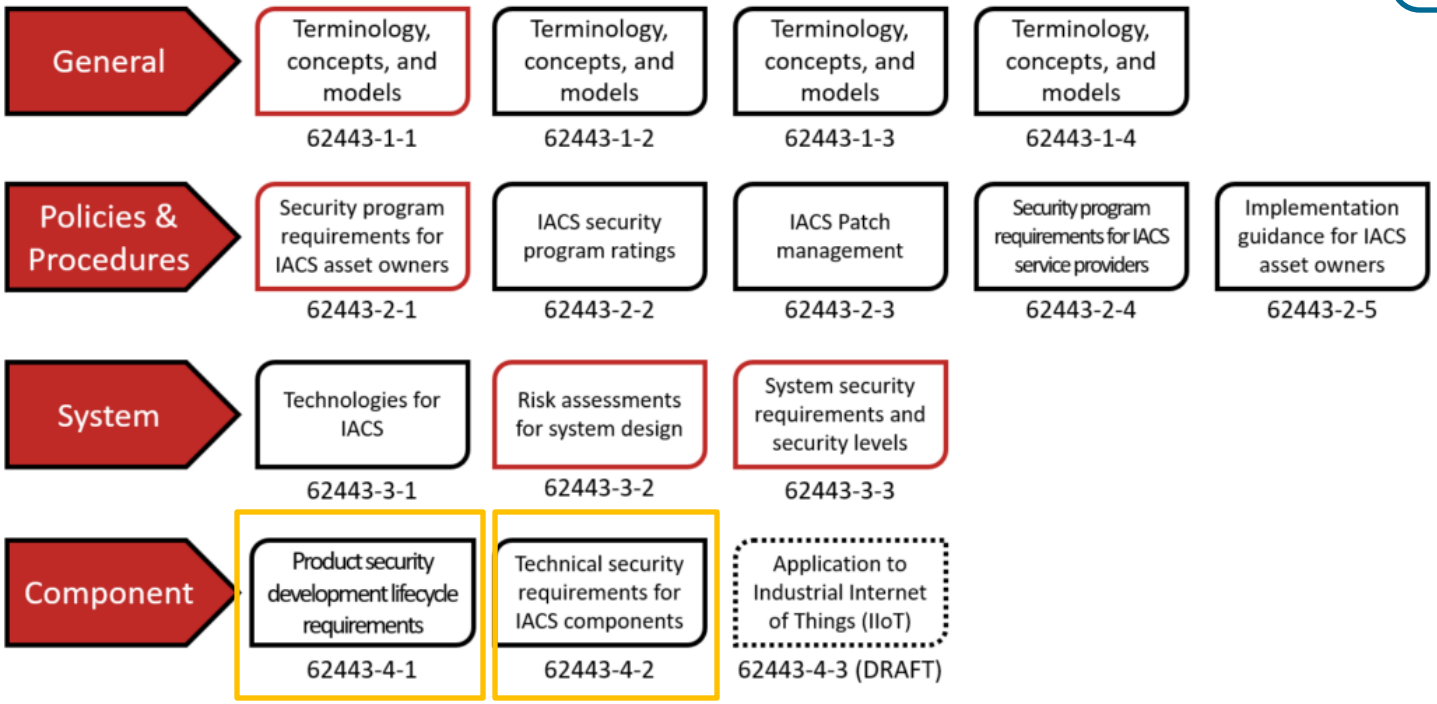
DistriNet


Mandatory Quality or Attainment
A level of Quality or Attainment
legislation
Standard
Product requirements
RED-DA
(August 2025)
Product Requirements + Product Lifecycle
CRA
(December 2027)
ETSI EN 303 645
requirements
IEC62443
requirements + lifecycle
Common Criteria
requirements + lifecycle
EN 18031
requirements
???
requirements + lifecycle


CRA
(December 2027)
IEC62443
Common Criteria


CRA
(December 2027)
IEC62443
Common Criteria

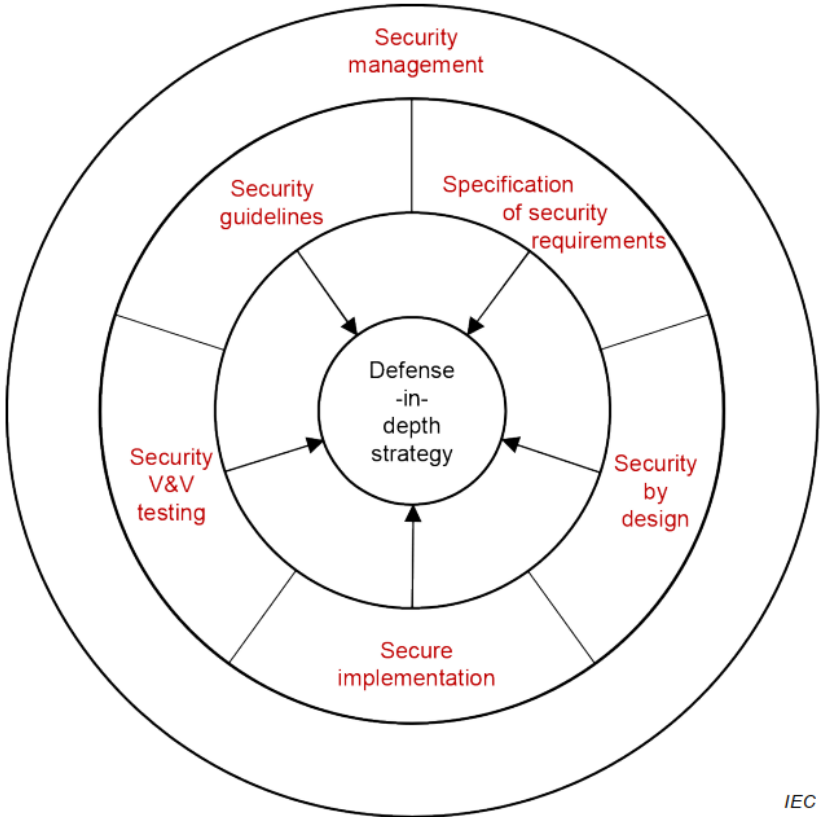
IEC62443



DistriNet

IEC62443-4-1: SDLC Requirements

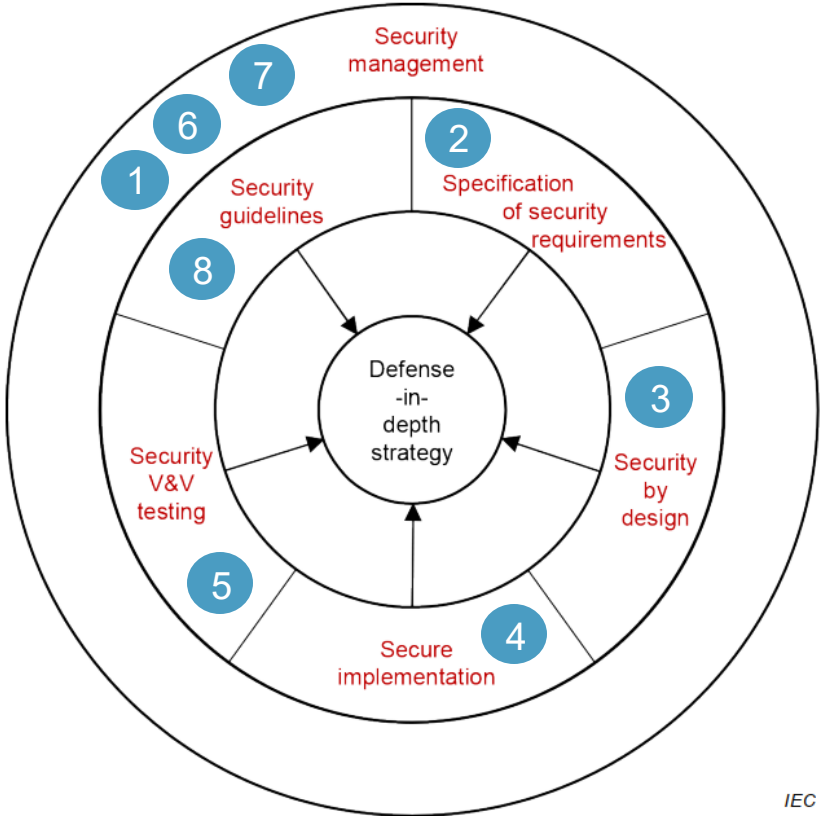
IEC62443



IEC62443-4-1: SDLC Requirements

IEC62443

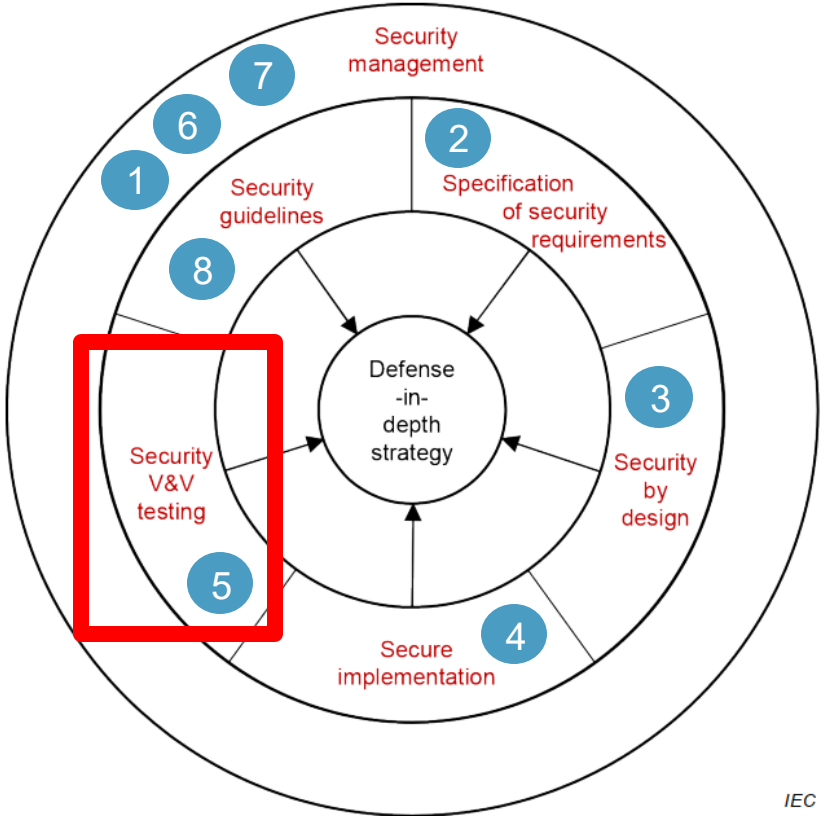
1. *Security management*
2. Specification of security requirements
3. Security by design
4. Secure implementation
5. Security verification and validation
6. *Management of security-related issues*
7. *Security update management*
8. Security guidelines



IEC62443-4-1: SDLC Requirements

IEC62443

1. *Security management*
2. Specification of security requirements
3. Security by design
4. Secure implementation
5. **Security verification and validation**
6. *Management of security-related issues*
7. *Security update management*
8. Security guidelines



IEC62443-4-1 – practice 5: Security verification and validation testing

- **SVV-1: Security requirements testing**
  - Functional testing of security requirements
  - Performance and scalability testing
- **SVV-2: Threat mitigation testing**
  - Test effectiveness of mitigations to threats identified by the threat model (STRIDE)
  - If a layered defense strategy is used, then test the effectiveness of each layer

Do security measures work?

- **SVV-3: Vulnerability Testing**
  - Base known vulnerability testing on public source for known vulnerabilities
  - Attack surface analysis, (un)known vulnerability scanning (fuzzing, stress testing…)
- **SVV-4: Penetration Testing**
  - Approach testing like an attacker
  - Often involves exploiting chained vulnerabilities in a product

Any code Vulnerabilities?

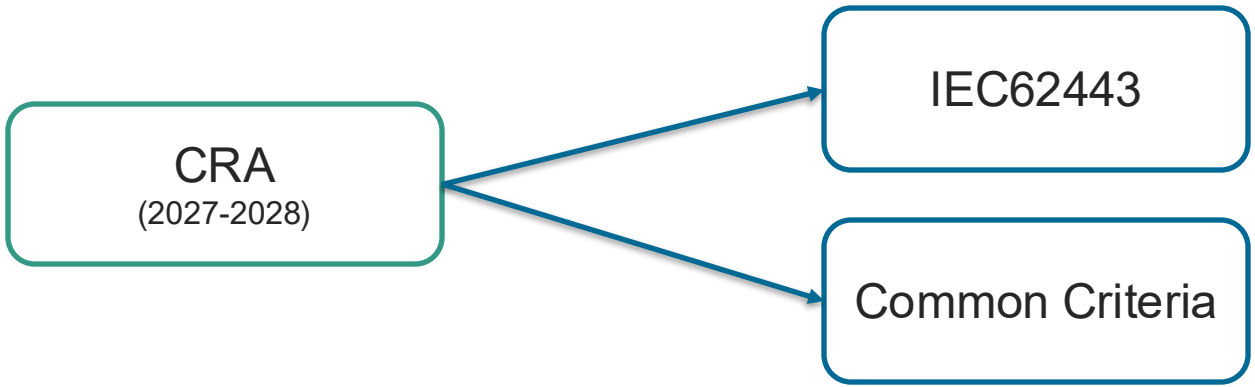
IEC62443-4-1 – practice 5: Security V&V testing

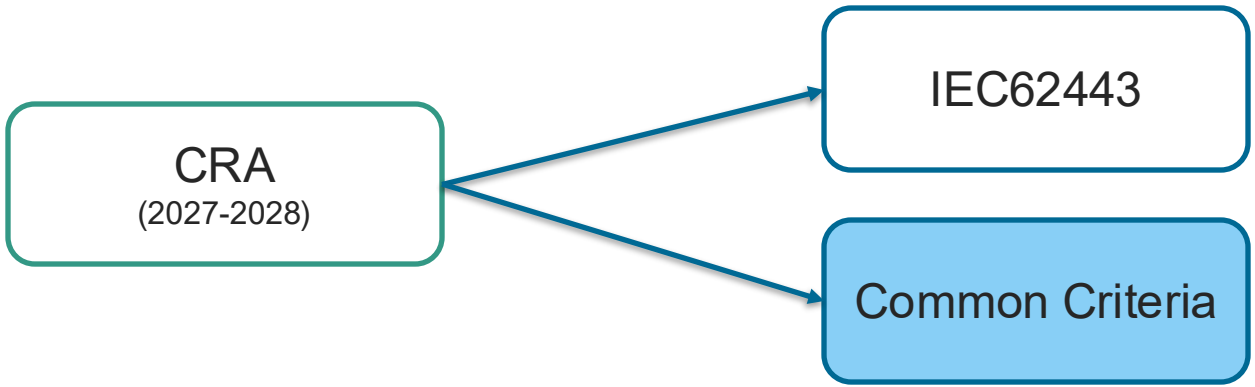
IEC62443

Table 3 – Required level of independence of testers from developers

Test type	Reference	Level of independence
Security requirements testing	SVV-1 – Security requirements testing	Independent department
Threat mitigation testing	SVV-2 – Threat mitigation testing	Independent department
Abuse case testing	SVV-3 – Vulnerability testing	Independent person
Static code analysis	SI-1 – Security implementation review	None
Attack surface analysis	SVV-3 – Vulnerability testing	Independent person
Known vulnerability scanning	SVV-3 – Vulnerability testing	Independent person
Software composition analysis	SVV-3 – Vulnerability testing	None
Penetration testing	SVV-4 – Penetration testing	Independent department or organization

Who should perform tests?


CRA
(2027-2028)
IEC62443
Common Criteria


CRA
(2027-2028)
IEC62443
Common Criteria

Common Criteria for IT Security Evaluation

ISO/IEC 15408

Common Criteria

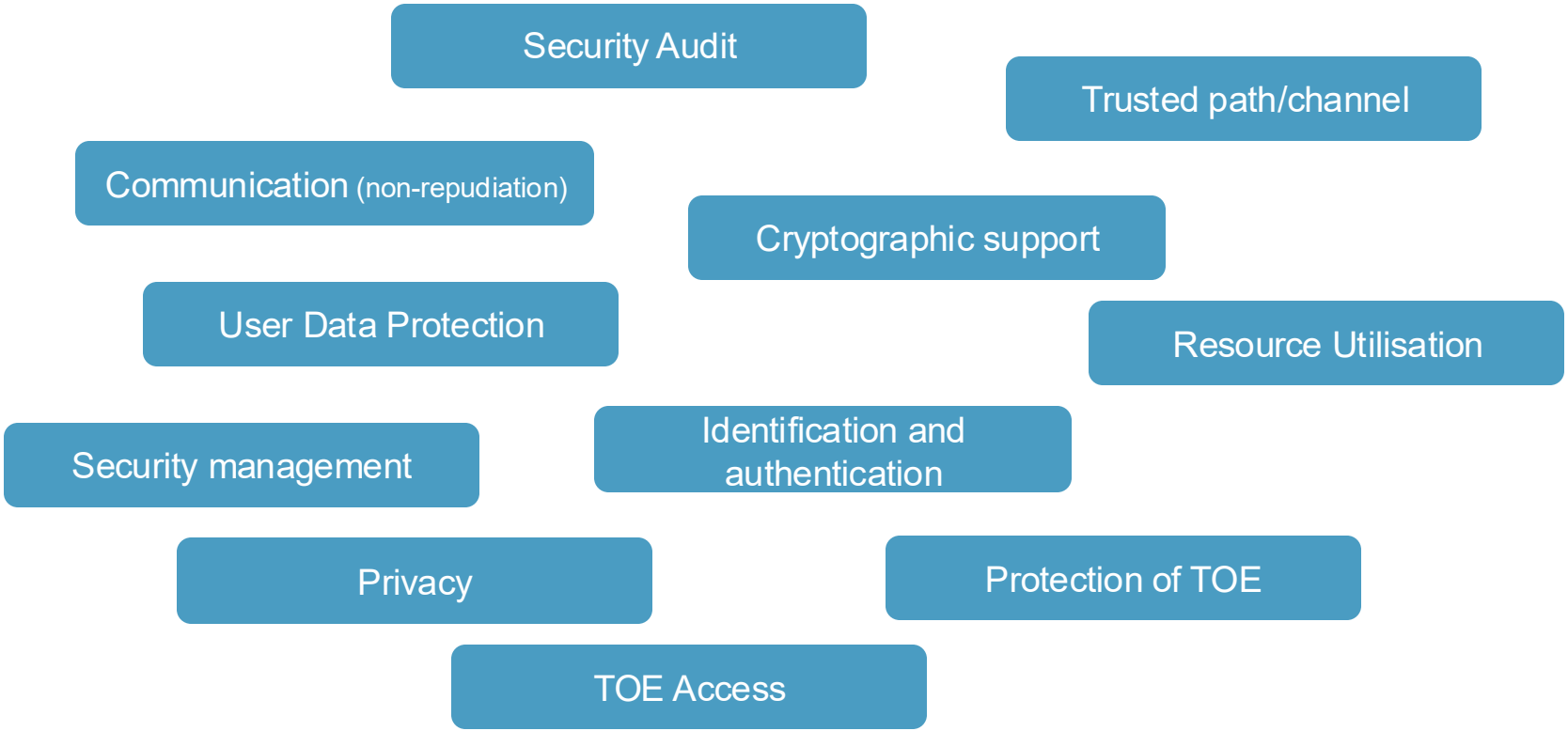
- a **framework** in which computer system **users** can specify their security **functional requirements (SFRs) and assurance requirements (SARs)** in a **Security Target** (ST), and may be taken from **Protection Profiles** (PPs)

- **Vendors** can then *implement* or **make claims about the security attributes of their products**, and testing laboratories can *evaluate* the products

DistriNet

Security Functional Requirement (SFR) Classes

Common Criteria



DistriNet

Security Assurance Requirement (SAR) Classes

Common Criteria

Protection Profile Configuration evaluation

Life-cycle support

Protection Profile evaluation

Tests

Class AGD: Guidance documents

Security Target evaluation

Composition

Development

Vulnerability assessment

DistriNet

Security Assurance Requirement (SAR) Classes

Common Criteria

Protection Profile Configuration evaluation

Life-cycle support

Protection Profile evaluation

Tests

Class AGD: Guidance documents

Security Target evaluation

Composition

Development

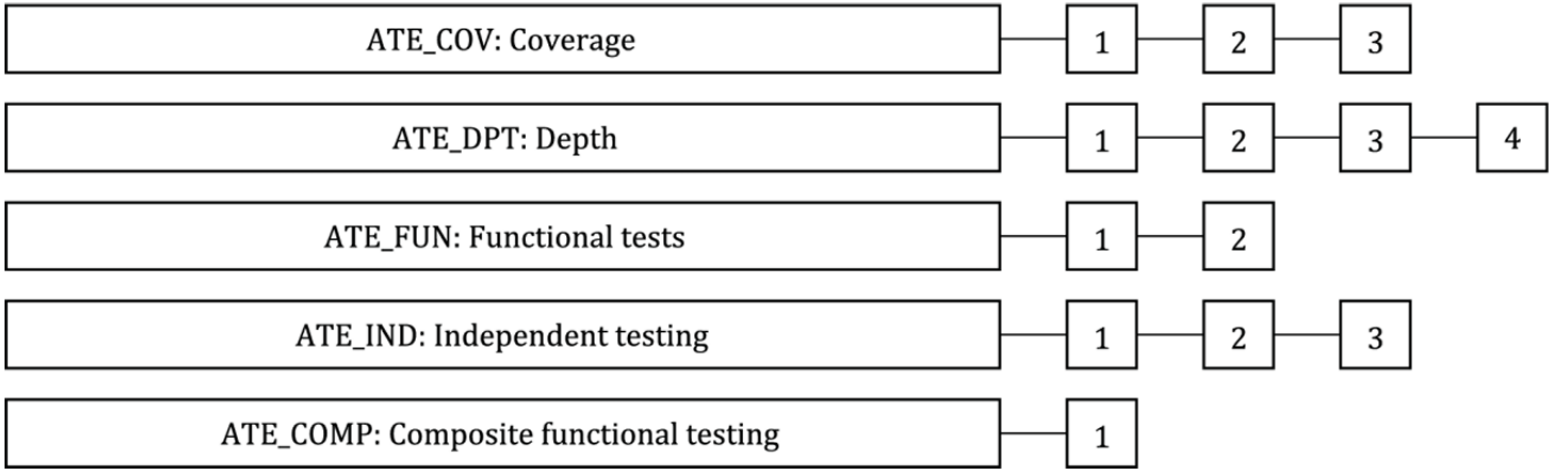
Vulnerability assessment

DistriNet

Security Assurance Requirement Class Tests

Common Criteria

- Focus on confirmation that the TSF operates according to its design descriptions
- This class does not address penetration testing
- Tests performed by developer and evaluator



Do security measures work?

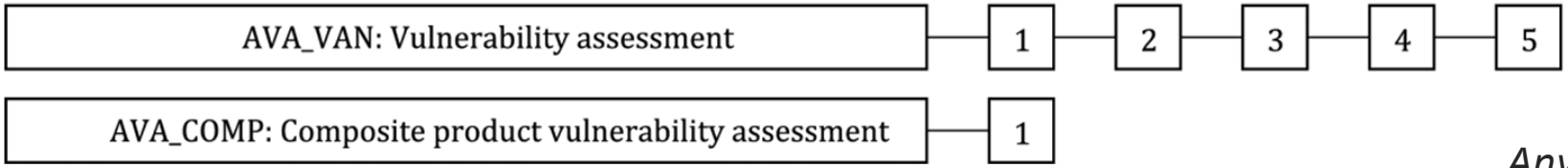
Who should perform tests?

DistriNet

SAR Class Vulnerability Assessment

Common Criteria

- addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the security target



Any code Vulnerabilities?

DistriNet

Conclusions

Mandatory Quality or Attainment

A level of Quality or Attainment

legislation

Standard

Certification

Evaluating the Quality or Attainment

Mandatory Quality or Attainment

A level of Quality or Attainment

legislation

Standard

Certification

Evaluating the Quality or Attainment

Mandatory Quality or Attainment

A level of Quality or Attainment

legislation

Standard

Certification

Evaluating the Quality or Attainment