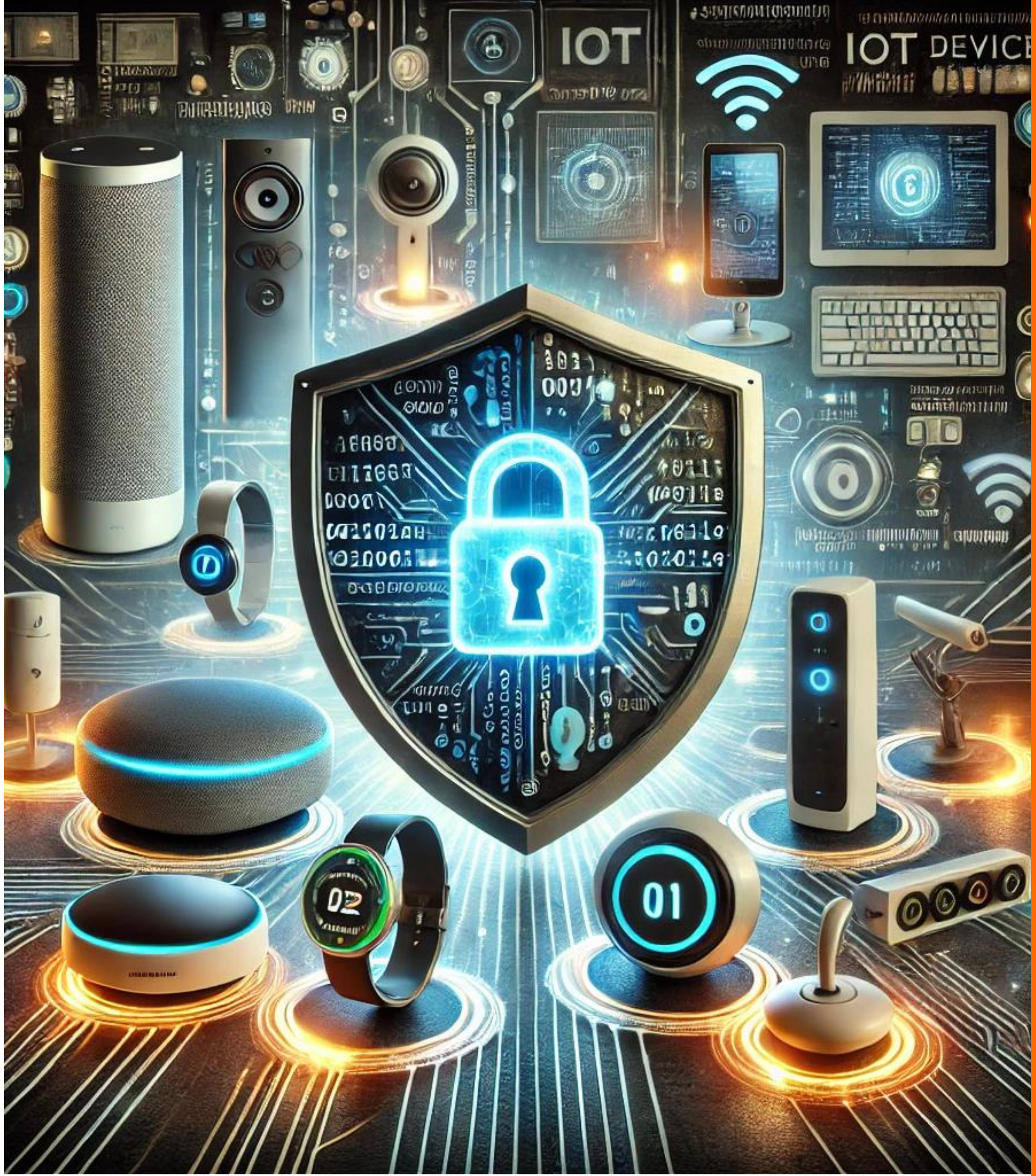
Applus laboratories

EN 18031: Understanding Standard

Common security requirements for radio equipment: Parts 1, 2, and 3

- December 2024
- **Nuria Carrió**



AGENDA

01 INTRODUCTION

EN 18031 is a European standard under development that aims to establish baseline security requirements for internet-connected consumer products and radio equipment to enhance their cybersecurity and protect users against threats like unauthorized access, data breaches, and malicious activities.

02 APPLICATION

EN 18031 is applied to a wide range of internet-connected radio equipment, including smart home devices, wearable technology, toys with wireless connectivity, and other consumer products that transmit or receive radio signals and connect to the internet.

03 ASSESSMENT

The assessment process in EN 18031 combines clear, objective requirements with a technology-agnostic approach, allowing manufacturers flexibility in their implementations. Compliance is demonstrated through documentation detailing how requirements are met, serving as input for testing to verify the actual security of the equipment.

04 REQUIREMENTS

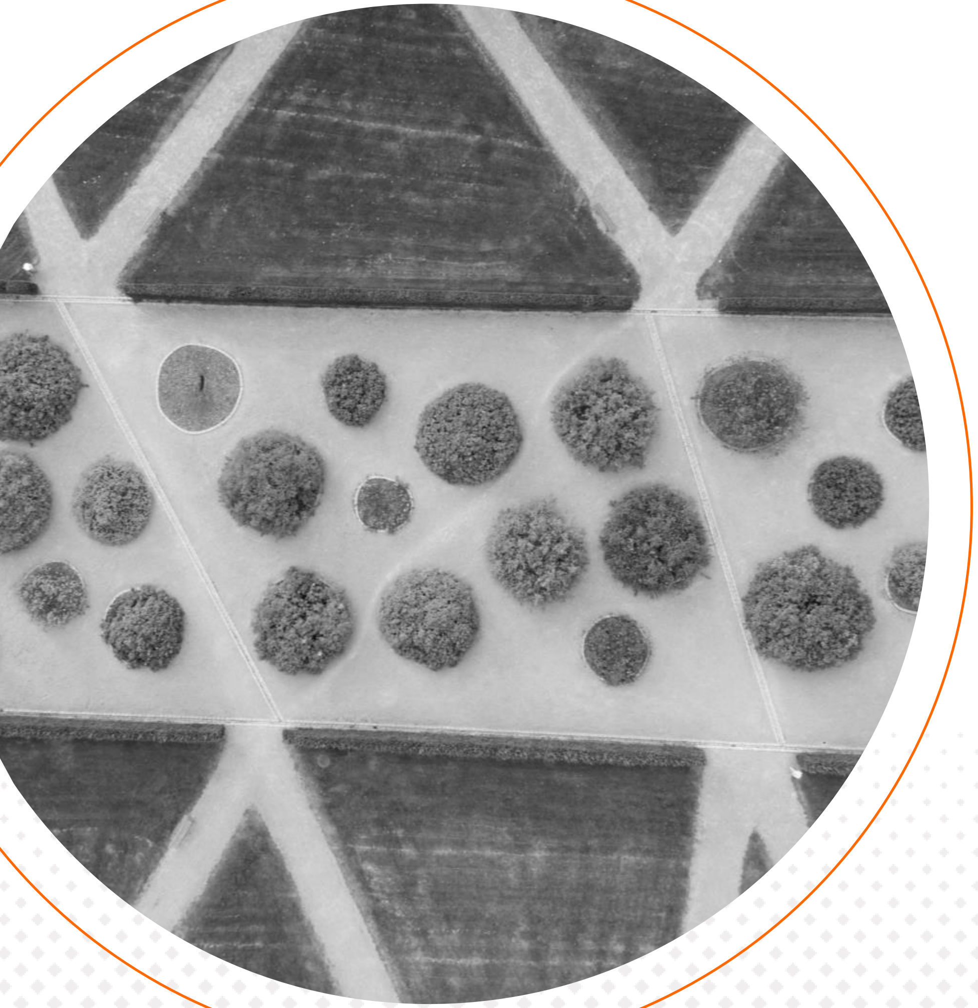
EN 18031 mandates that internet-connected radio equipment must implement essential security measures to protect network integrity, user data confidentiality, and financial transaction security. The standard also specifies requirements for hardware security.

05 MAPPING

EN 18031 demonstrates how complying with the security provisions of ETSI EN 303 645 can serve as a helpful framework for radio equipment manufacturers to meet the corresponding security requirements outlined in EN 18031.

06 CONCLUSION

EN 18031 provides a comprehensive set of cybersecurity requirements aimed at mitigating the risks associated with internet-connected radio equipment, enhancing overall product security, and protecting user privacy and financial data throughout the equipment's lifecycle.



01 INTRODUCTION

EN 18031 is a European standard under development that aims to establish baseline security requirements for internet-connected consumer products and radio equipment to enhance their cybersecurity and protect users against threats like unauthorized access, data breaches, and malicious activities.

European foreword

- The **standard EN 18031** has been prepared by Technical Committee CEN/CENELEC JTC 13 “Cybersecurity and Data Protection” .
- Support essential requirements of the Regulation (EU) 2022/30 supplementing **Directive 2014/53/EU** of the European Parliament and of the Council.
- Application of the essential requirements referred to in **Article 3(3), points (d) (e) and (f), of that Directive**.

The standard consist in three parts covering the different RED cyber articles 3.3(d,e,f):

EN 18031-1

RED: 3.3 (d)
Ensure network protections: not harm the network nor misuse network resources

Common security requirements for general internet-connected radio equipment

Applicable to: all internet connected radio equipment.

Addressing security and network risks inherent in such devices

EN 18031-2

RED: 3.3 (e)
Ensure protection of personal data and privacy of the user / subscriber

Focused on radio equipment that processes personal, traffic, or location data.

Applicable to: all internet connected radio equipment, Childcare radio equipment, Toys radio equipment and Wearable radio equipment.

Addressing specific security and privacy risks associated with these devices.

EN 18031-3

RED: 3.3 (f)
Ensure protection from fraud

Focused on Internet connected radio equipment processing virtual money or monetary value.

Applicable to: devices that transfer money, monetary value, or virtual currency.

Addressing security and financial risks inherent in such devices.

- RED-DA Will become mandatory on **August 1st, 2025**.
- Currently **NOT** harmonized.
- Probably will be harmonized with restrictions.

- The security requirements presented in this **baseline EN 18031 standard** are developed to improve the ability of radio equipment to protect its assets against common cybersecurity threats and to mitigate publicly known exploitable vulnerabilities.

- The **EN 18031 standard** provides the guidance material including lists of examples. These examples given are only indicative possibilities, as there are other possibilities that are not listed, and even using the examples given will not be sufficient unless the mechanisms and measures chosen are implemented in a coordinated fashion.

02 APPLICATION

EN 18031 is applied to a wide range of internet-connected radio equipment, including smart home devices, wearable technology, toys with wireless connectivity, and other consumer products that transmit or receive radio signals and connect to the internet.

Security mechanism: Fundamental concept

- This standard uses the **concept of mechanisms** to instruct the user of this standard when to apply certain **security measures**.

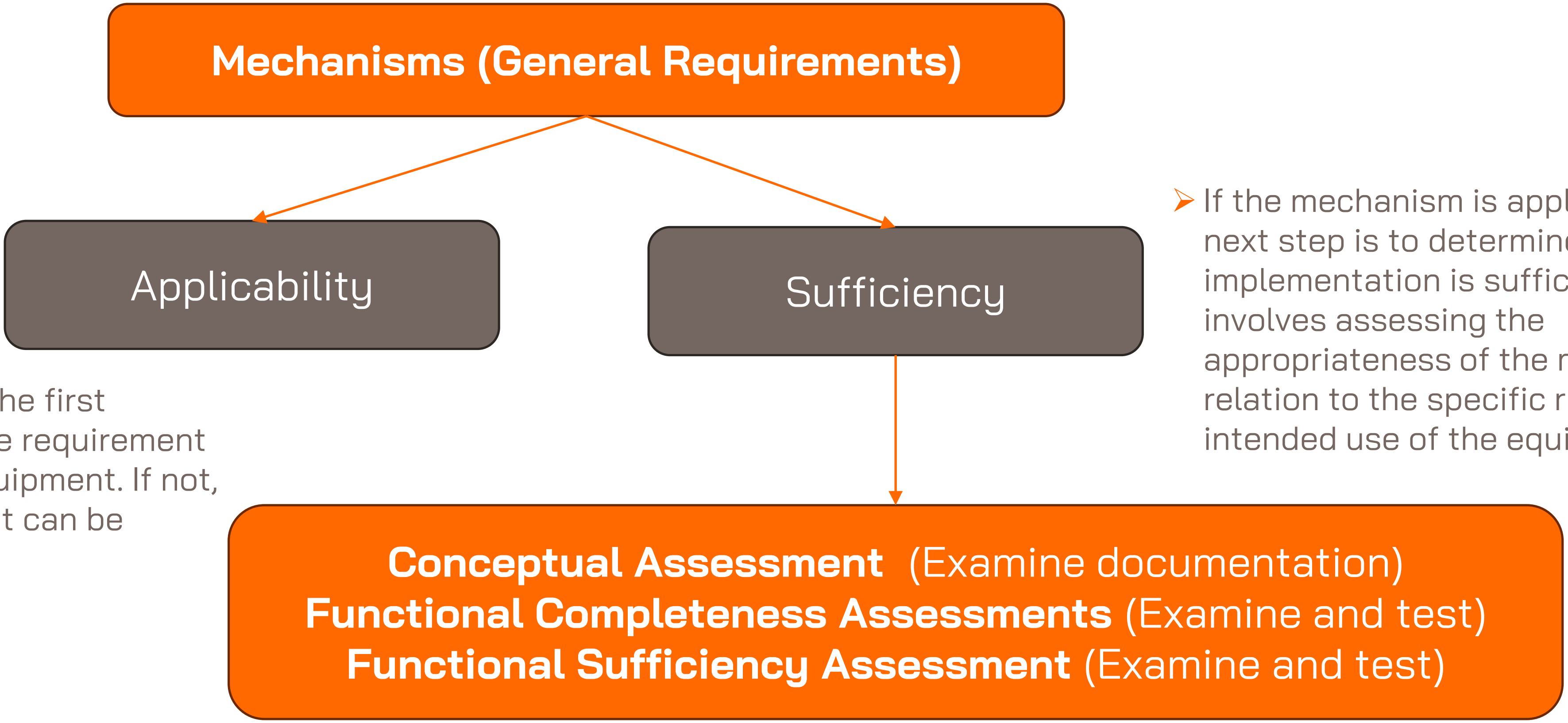
- Mechanisms address the **applicability and sufficiency through** a set of requirements including **assessment criteria**.

- An applicable/non-applicable decision is taken for each of the mechanisms specified. If the mechanism is applicable, it is followed by a PASS/FAIL decision for each individual assessment including **conceptual, and functional assessments** for **documentation completeness and implementation sufficiency**.

EN 18031 Standard: Flexibility & specificity in a horizontal standard

- **Mechanisms, Not Solutions**
  - ➢ The standard focuses on security mechanisms (e.g., encryption, access control) rather than dictating specific solutions. This allows manufacturers to tailor their implementations to the unique characteristics of their products and intended uses.
- **Wide Range of Products and Use Cases**
  - ➢ This is a horizontal standard, meaning it applies to a broad range of internet-connected radio equipment. This diversity necessitates a flexible approach.
- **Adapting to Context**
  - ➢ The appropriateness and strength of security measures depend heavily on the specific equipment and its intended use. A strong security measure for a high-risk device might be overkill for a simple sensor, and vice-versa.
- **Constraints and Guidance**
  - ➢ The standard provides specific constraints (requirements) and assessment questions to guide manufacturers in choosing the right mechanisms and their level of implementation. This prevents them from solely relying on their own judgment, which might not be sufficient to address all security concerns.

APPLICATION | Security mechanism: Fundamental concept



Mechanisms (General Requirements)

Applicability

Sufficiency

Conceptual Assessment (Examine documentation)
Functional Completeness Assessments (Examine and test)
Functional Sufficiency Assessment (Examine and test)

- For each mechanism, the first question is whether the requirement is applicable to the equipment. If not, the related assessment can be skipped.

- If the mechanism is applicable, the next step is to determine if its implementation is sufficient. This involves assessing the appropriateness of the mechanism in relation to the specific risks and intended use of the equipment.

- This decision process is applied to each individual item or aspect of the equipment. For example, the need for a particular security mechanism might be different for each external interface on the device.

03 ASSESSMENT

The assessment process in EN 18031 combines clear, objective requirements with a technology-agnostic approach, allowing manufacturers flexibility in their implementations. Compliance is demonstrated through documentation detailing how requirements are met, serving as input for testing to verify the actual security of the equipment.

APPLICATION

EN 18031 Standard: Flexibility & specificity in a horizontal standard

- **Risk-Based Approach**: All parts emphasize a risk-based approach, requiring **manufacturers** to assess and mitigate cybersecurity risks throughout the product lifecycle.

- **Documentation and Compliance**: Manufacturers must document their cybersecurity strategies and ensure that their products meet the specified standards before they are placed on the market.

- **Assessment and Testing**: The standard outlines methods for testing and validating the security features of radio equipment, including both self-assessment (not allowed at this moment) and third-party evaluation options.

Make a Risk Assessment, the first step!

- Manufacturer shall perform a **Cybersecurity Risk Assessment**:
  - For their devices.
  - To choose appropriate compliance procedures.
  - Example: STRIDE inside the standard, ETSI’s risk manag process…

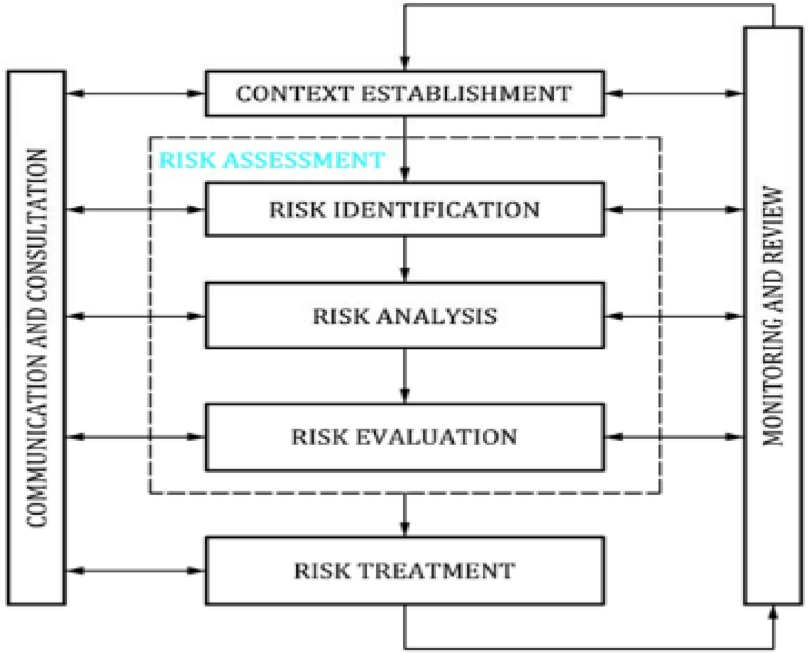


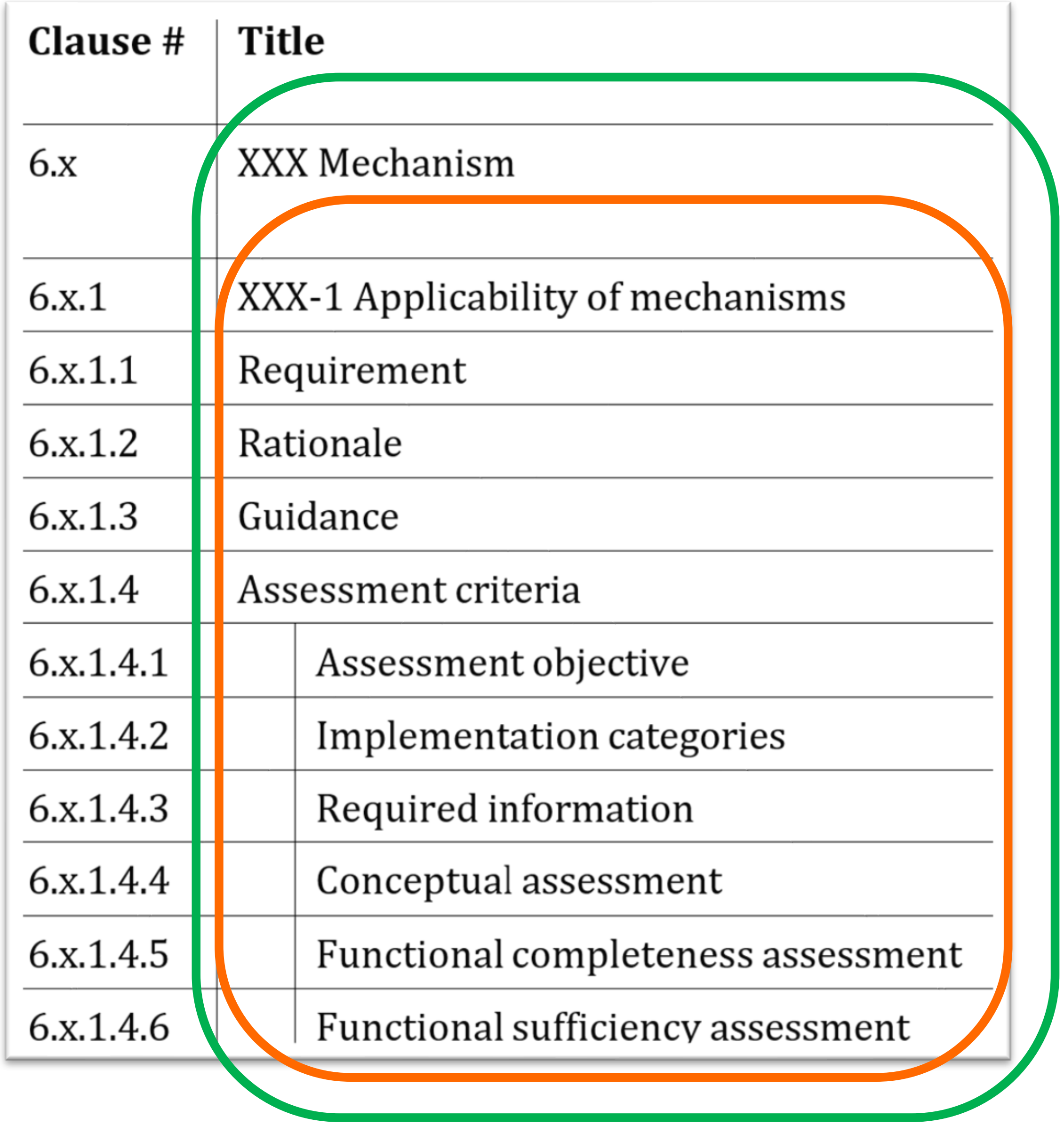
__Figure 1__ Risk management process in ISO/IEC 27000 series and ISO/IEC 31000 series

MANDATORY RISK ASSESSMENT TO BE PERFORMED by THE MANUFACTURER

OPTIONAL TO USE STRIDE METHOD

Security mechanism: Structure overview

- Clauses 6.x in EN 18031 (all parts)



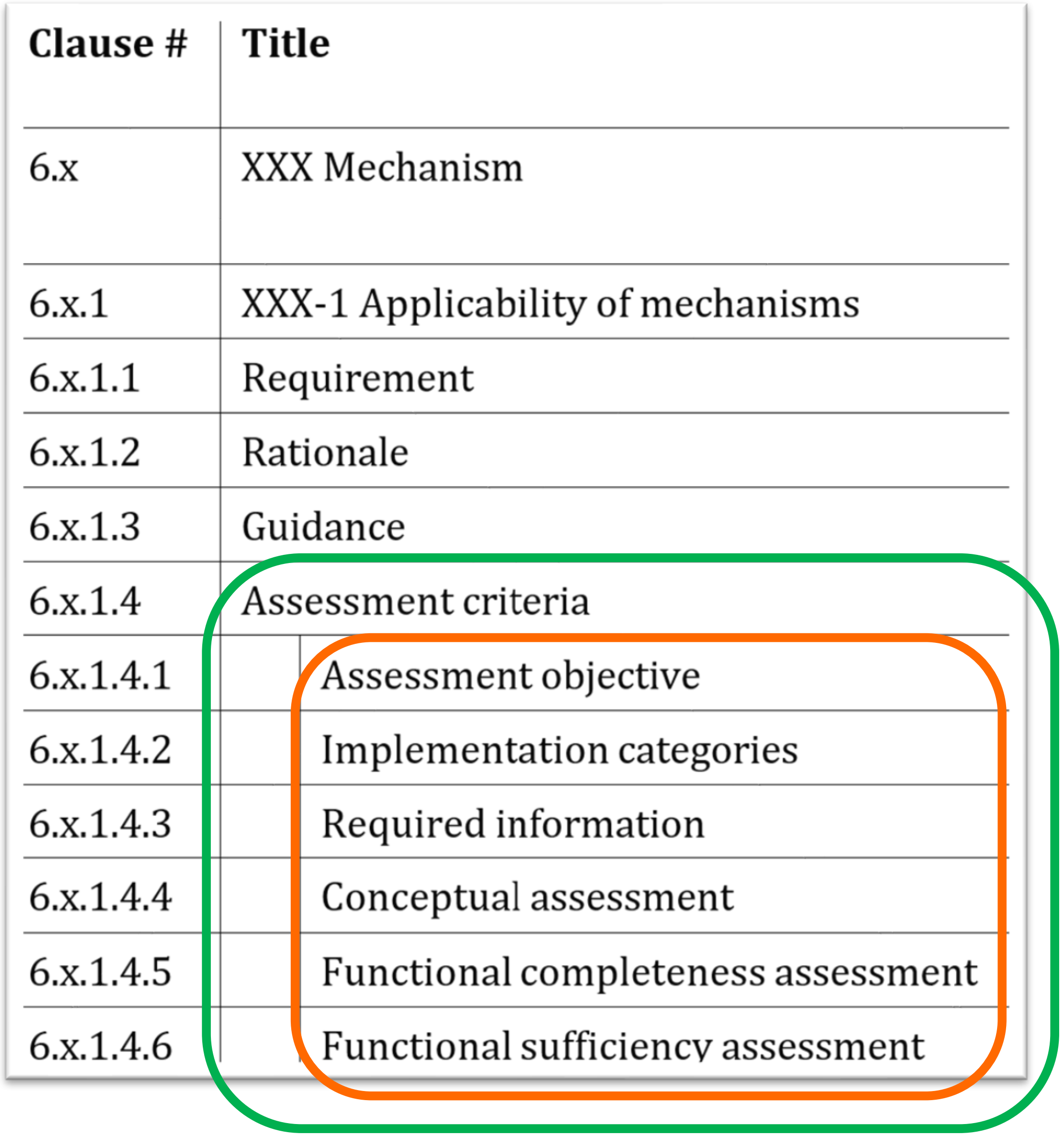
Clause #	Title
6.x	XXX Mechanism
6.x.1	XXX-1 Applicability of mechanisms
6.x.1.1	Requirement
6.x.1.2	Rationale
6.x.1.3	Guidance
6.x.1.4	Assessment criteria
6.x.1.4.1	Assessment objective
6.x.1.4.2	Implementation categories
6.x.1.4.3	Required information
6.x.1.4.4	Conceptual assessment
6.x.1.4.5	Functional completeness assessment
6.x.1.4.6	Functional sufficiency assessment

Security mechanism: Assessment approach

- **Assessment Approach**

➢ **Documentation Review:** Manufacturers must provide detailed **technical documentation** that describes the security measures they have implemented.

➢ **Testing:** The equipment undergoes **actual testing (functional testing + security testing)** to verify that it behaves as documented and meets the security objectives.

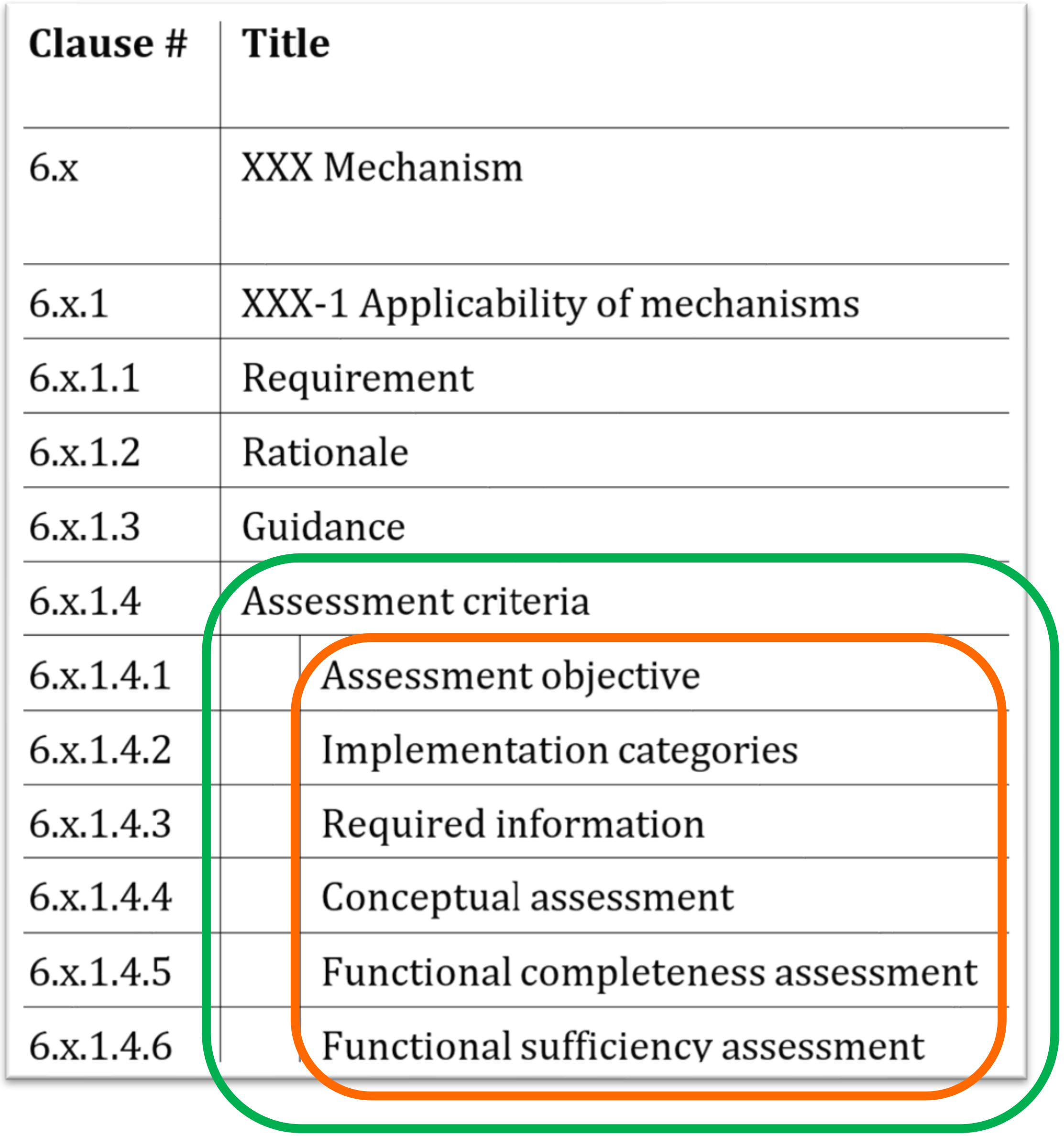


Clause #	Title
6.x	XXX Mechanism
6.x.1	XXX-1 Applicability of mechanisms
6.x.1.1	Requirement
6.x.1.2	Rationale
6.x.1.3	Guidance
6.x.1.4	Assessment criteria
6.x.1.4.1	Assessment objective
6.x.1.4.2	Implementation categories
6.x.1.4.3	Required information
6.x.1.4.4	Conceptual assessment
6.x.1.4.5	Functional completeness assessment
6.x.1.4.6	Functional sufficiency assessment

Security mechanism: Assessment criteria

Assessment Criteria

- **Precise and Objective Definitions:** The security measures outlined in EN 18031 are intentionally worded to be as clear and specific as possible. This avoids ambiguity and ensures a consistent understanding of what's expected from manufacturers.
- **Technology Agnostic:** The standard avoids dictating specific technologies or solutions. Instead, it focuses on the desired security outcomes, allowing manufacturers flexibility in how they achieve compliance.
- **Documentation for Compliance Testing:** To demonstrate compliance, manufacturers must provide detailed documentation explaining how they meet each requirement. This documentation will be used as input for compliance testing, which verifies if the product's implementation actually delivers the required security.



Clause #	Title
6.x	XXX Mechanism
6.x.1	XXX-1 Applicability of mechanisms
6.x.1.1	Requirement
6.x.1.2	Rationale
6.x.1.3	Guidance
6.x.1.4	Assessment criteria
6.x.1.4.1	Assessment objective
6.x.1.4.2	Implementation categories
6.x.1.4.3	Required information
6.x.1.4.4	Conceptual assessment
6.x.1.4.5	Functional completeness assessment
6.x.1.4.6	Functional sufficiency assessment

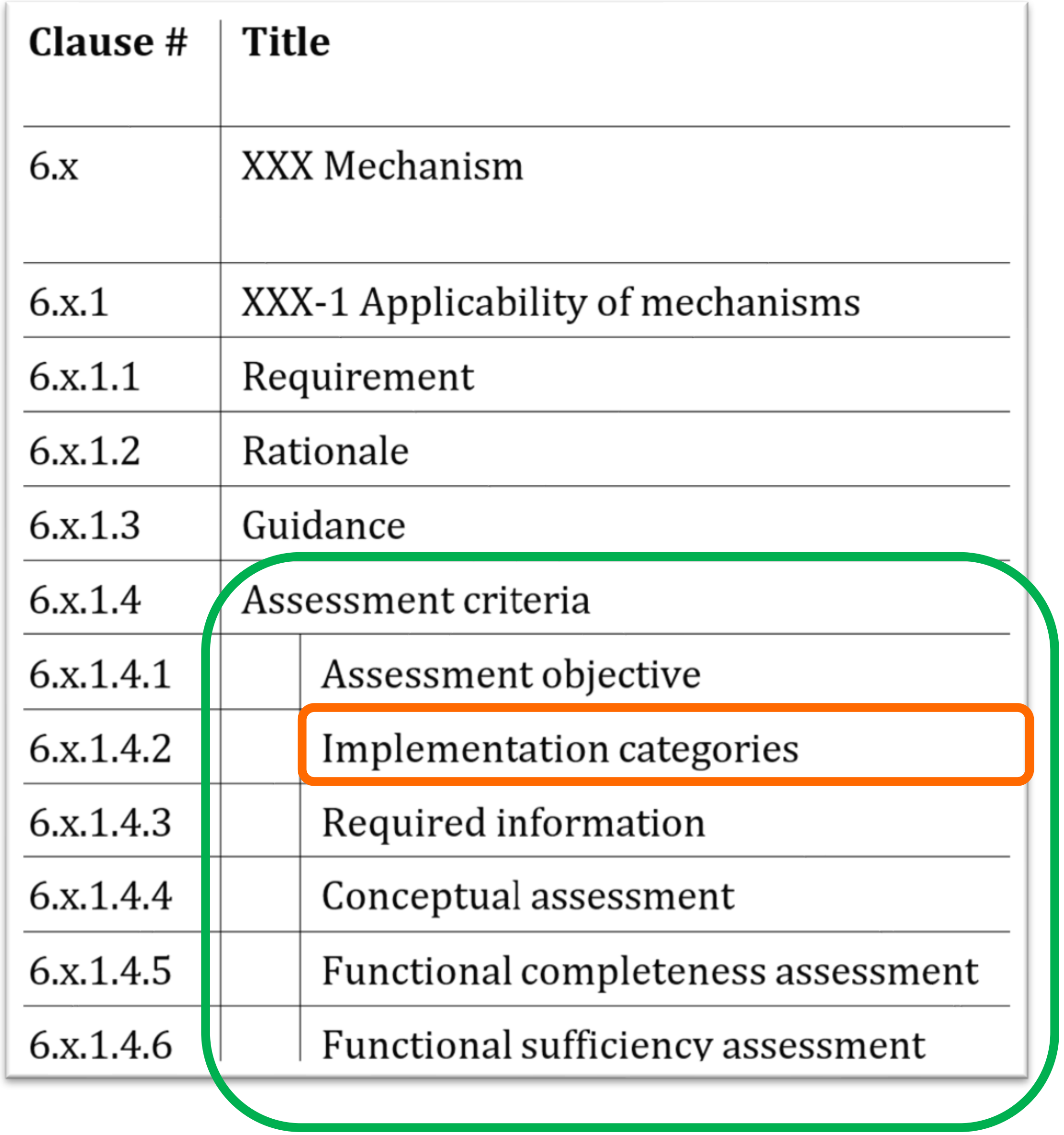
Security mechanism: Implementation categories

- **Common Technical Solutions**

➢ The standard recognizes that certain technical solutions are commonly used to meet the security requirements. These common solutions are grouped into "implementation categories.“

- **Implementation-Specific Assessment Units**

➢ For these common implementation categories, the standard provides specific assessment units (AUs) in addition to the generic ones. These implementation-specific AUs are tailored to evaluate the particular security mechanisms and technologies used within that category.



Clause #	Title
6.x	XXX Mechanism
6.x.1	XXX-1 Applicability of mechanisms
6.x.1.1	Requirement
6.x.1.2	Rationale
6.x.1.3	Guidance
6.x.1.4	Assessment criteria
6.x.1.4.1	Assessment objective
6.x.1.4.2	Implementation categories
6.x.1.4.3	Required information
6.x.1.4.4	Conceptual assessment
6.x.1.4.5	Functional completeness assessment
6.x.1.4.6	Functional sufficiency assessment

Security mechanism: Required Information

- **Information Elements (`E.Info.xxxxx`)**

➢ **`xxxxx`:** A code that identifies the specific information element, eg, `[E.Info.ACM-1.ACM]`, `[E.Info.AUM-1-1.ACM.NetworkInterface]`

- **Expected General Information**

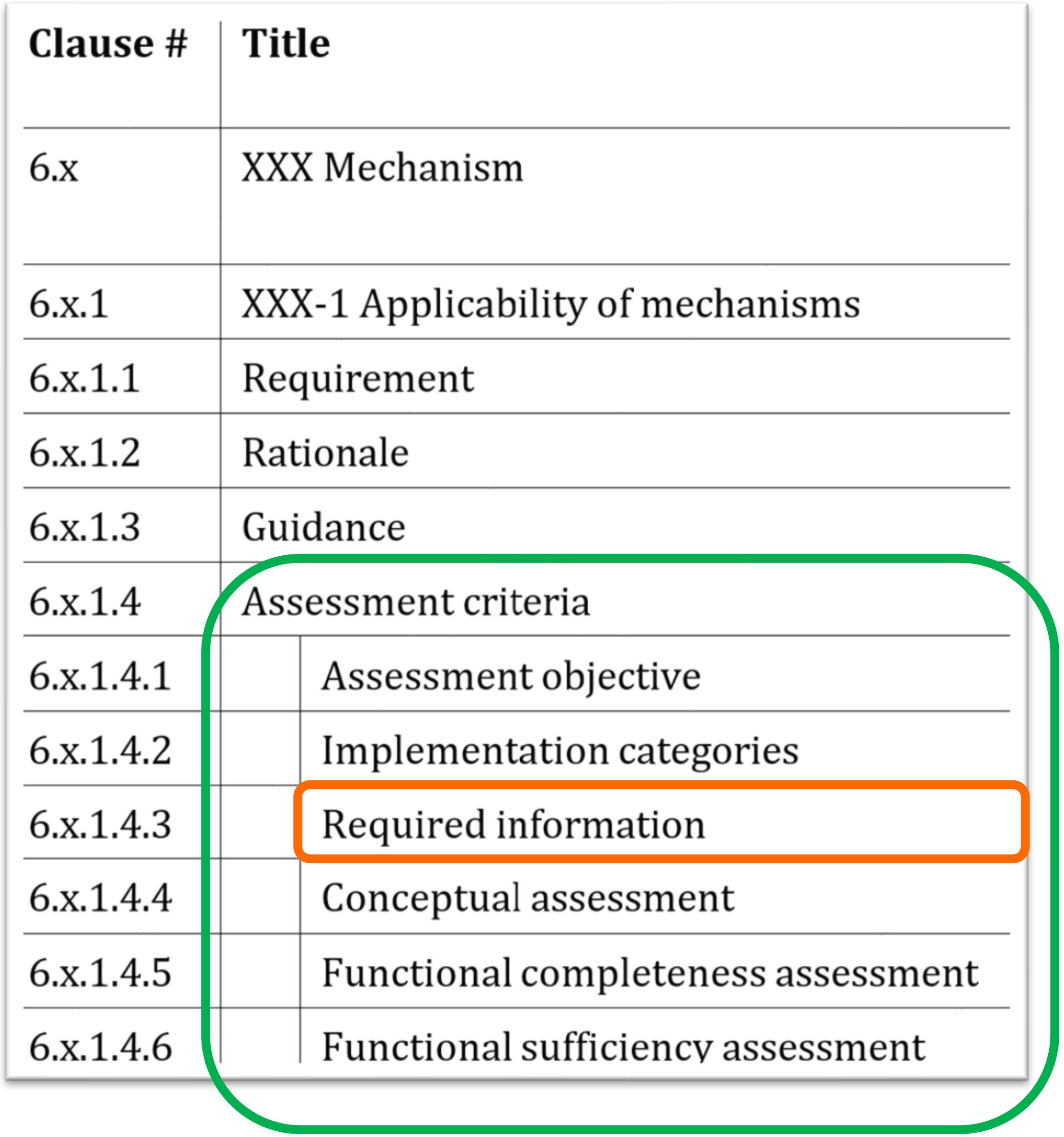
➢ Intended Equipment Functionality

➢ Technical Information

➢ Declared Best Practices

➢ Specific Details

➢ Security Risk Assessment



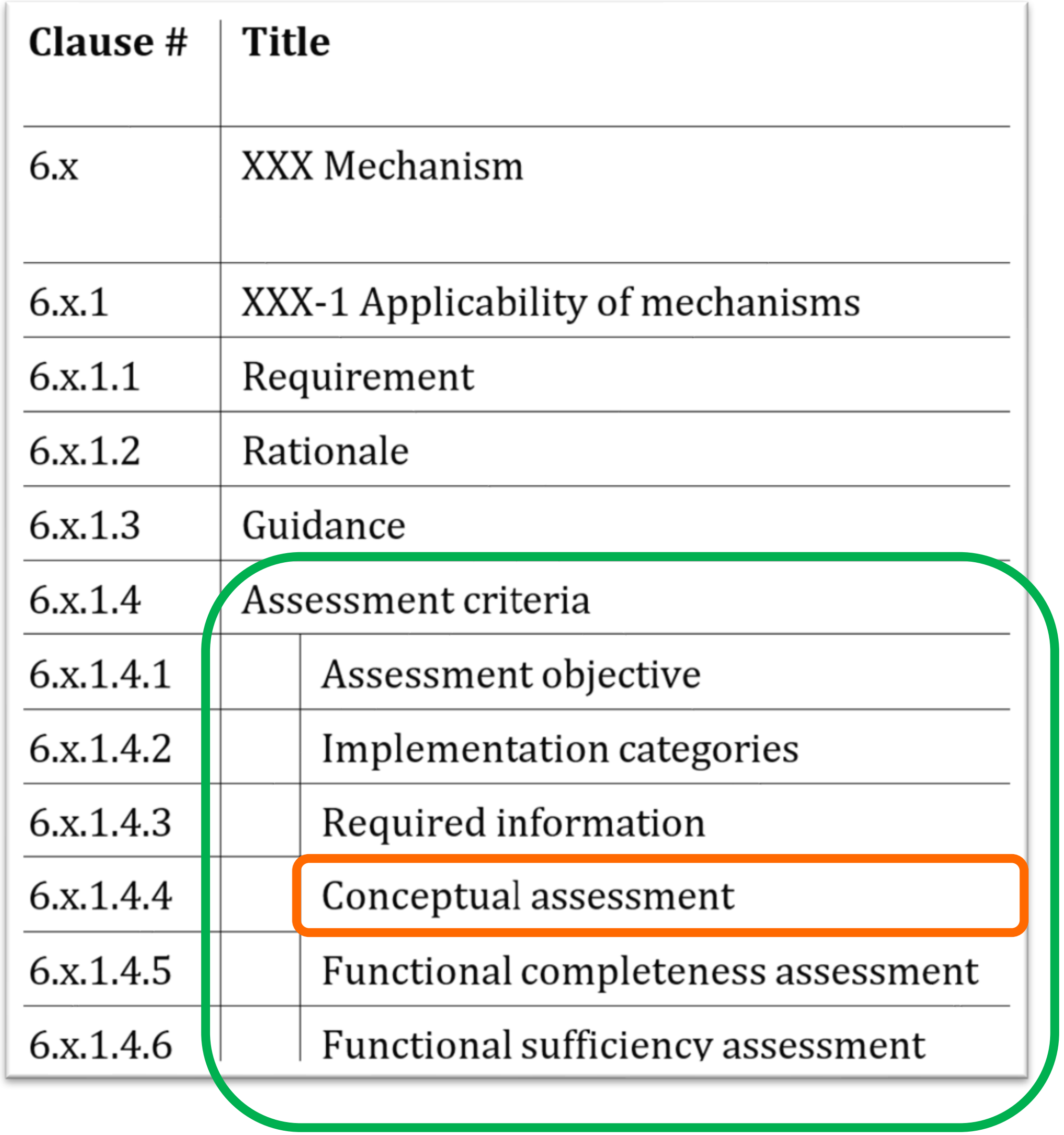
Clause #	Title
6.x	XXX Mechanism
6.x.1	XXX-1 Applicability of mechanisms
6.x.1.1	Requirement
6.x.1.2	Rationale
6.x.1.3	Guidance
6.x.1.4	Assessment criteria
6.x.1.4.1	Assessment objective
6.x.1.4.2	Implementation categories
6.x.1.4.3	Required information
6.x.1.4.4	Conceptual assessment
6.x.1.4.5	Functional completeness assessment
6.x.1.4.6	Functional sufficiency assessment

Security mechanism: Conceptual assessment (1/3)

- **Conceptual Assessment (Documentation Review)**

➢ **Evidence Evaluation:** The evaluator carefully examines the documentation to see if it clearly explains the chosen security mechanisms, their implementation details, and why certain choices were made.

➢ **Justification Evaluation (Decision Tree):** The evaluator assesses the manufacturer's reasoning for applying (or not applying) certain security mechanisms to specific interfaces or assets.

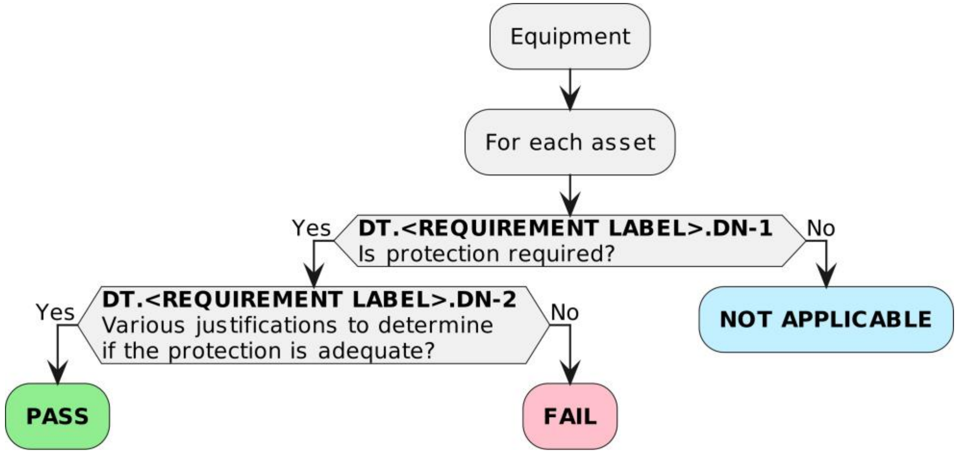


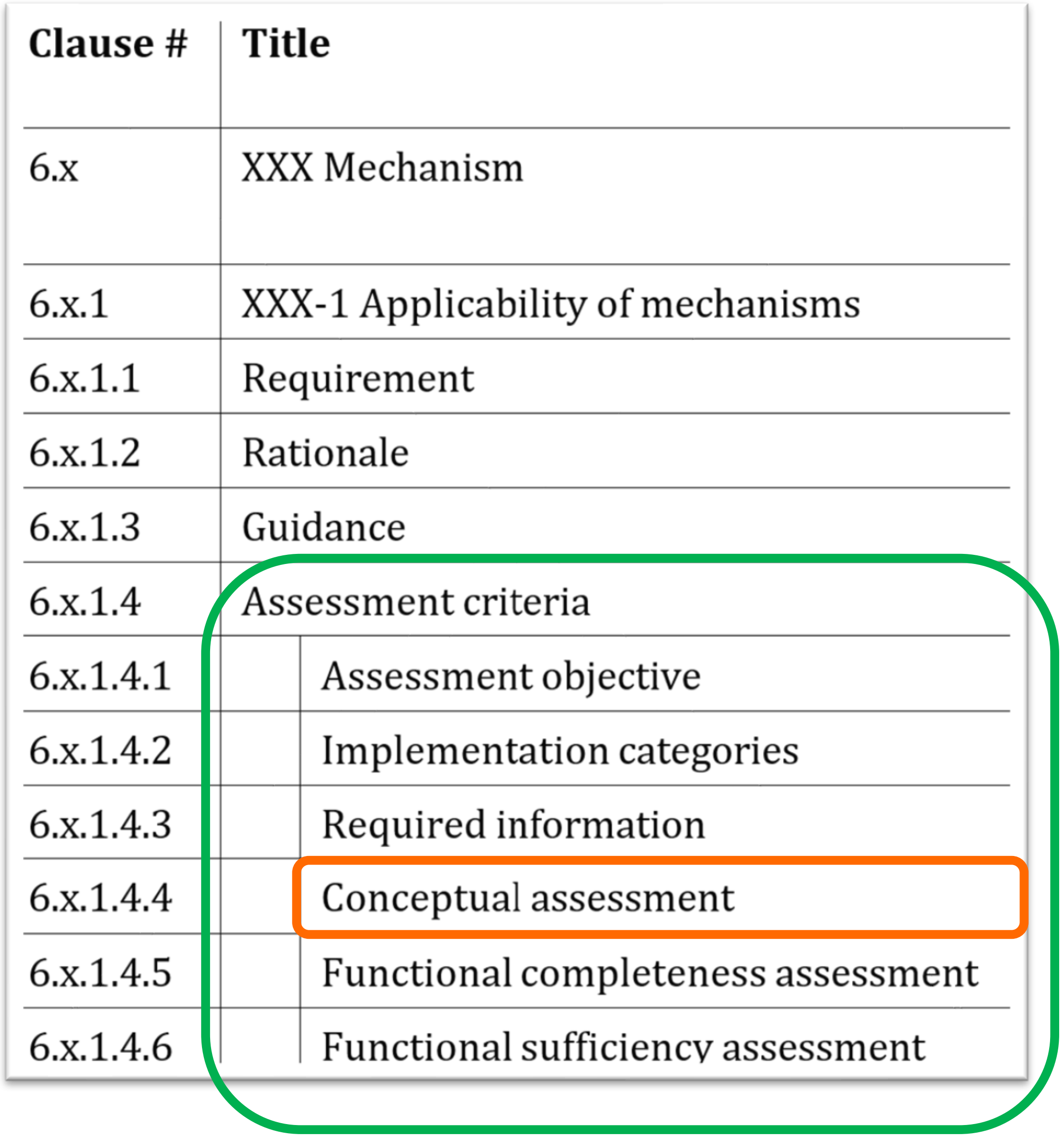
Clause #	Title
6.x	XXX Mechanism
6.x.1	XXX-1 Applicability of mechanisms
6.x.1.1	Requirement
6.x.1.2	Rationale
6.x.1.3	Guidance
6.x.1.4	Assessment criteria
6.x.1.4.1	Assessment objective
6.x.1.4.2	Implementation categories
6.x.1.4.3	Required information
6.x.1.4.4	Conceptual assessment
6.x.1.4.5	Functional completeness assessment
6.x.1.4.6	Functional sufficiency assessment

Security mechanism: Conceptual assessment: Decision Tree (2/3)

- **Justification Evaluation (Decision Tree)**

➢ **Guide Security Assessments:** Decision trees help determine if specific security requirements are applicable and, if so, whether the implemented protection is adequate for a particular piece of equipment and its intended use.


Equipment
For each asset
Yes
DT.<REQUIREMENT LABEL>.DN-1
Is protection required?
No
NOT APPLICABLE
Yes
DT.<REQUIREMENT LABEL>.DN-2
Various justifications to determine if the protection is adequate?
No
PASS
FAIL



Clause #	Title
6.x	XXX Mechanism
6.x.1	XXX-1 Applicability of mechanisms
6.x.1.1	Requirement
6.x.1.2	Rationale
6.x.1.3	Guidance
6.x.1.4	Assessment criteria
6.x.1.4.1	Assessment objective
6.x.1.4.2	Implementation categories
6.x.1.4.3	Required information
6.x.1.4.4	Conceptual assessment
6.x.1.4.5	Functional completeness assessment
6.x.1.4.6	Functional sufficiency assessment

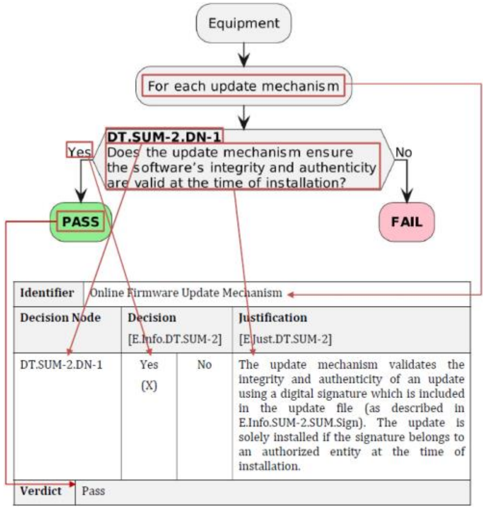
Security mechanism: Conceptual assessment: Decision Tree (3/3)

- **Justification Evaluation (Decision Tree)**

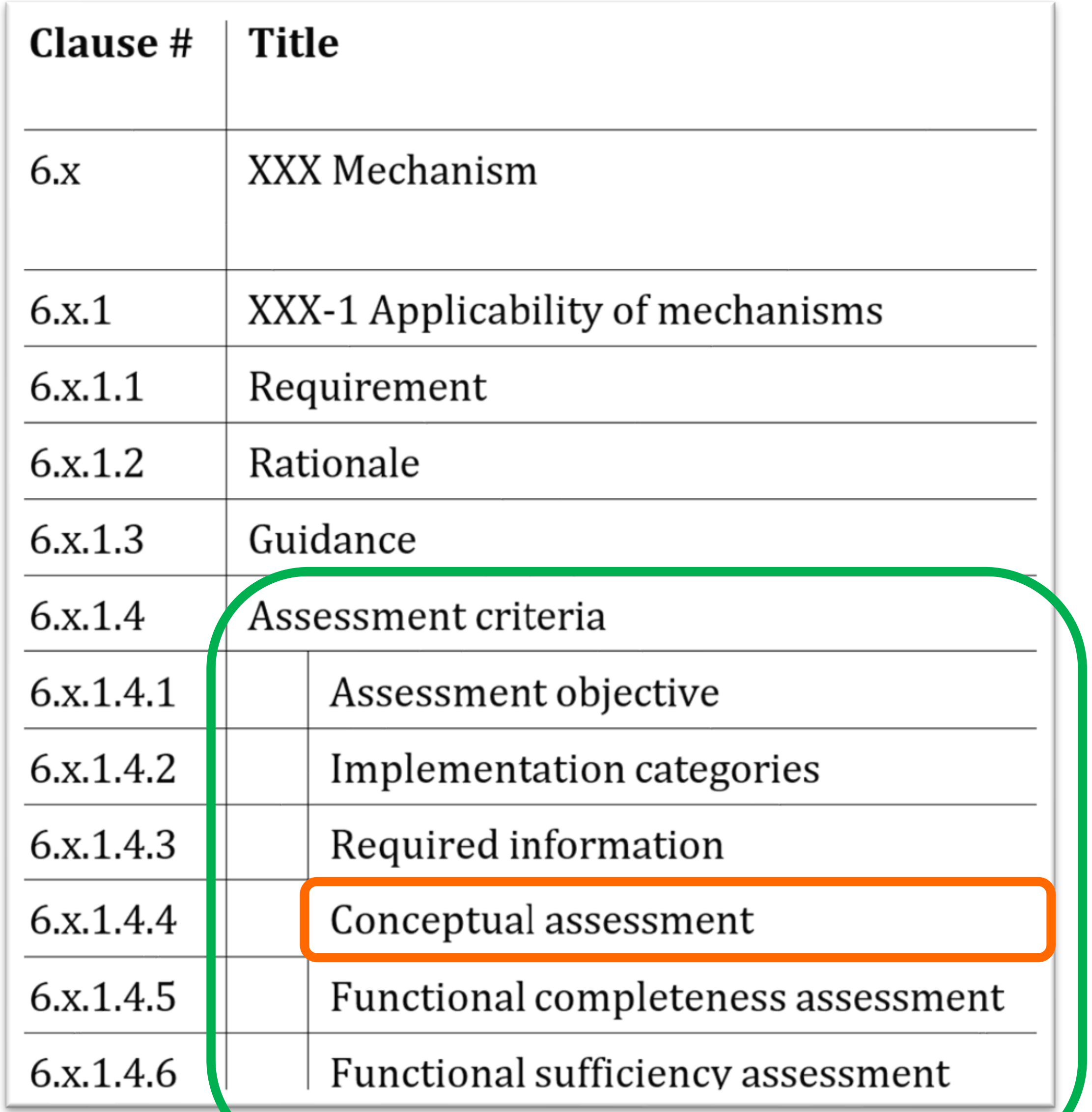
➢ **Justification of Decisions (YES/NO):**

✓ **YES:** Justification is based on evidence that the protection measures effectively mitigate the risks associated with the specific asset and its intended use.

✓ **NO:** Justification is based on evidence that the protection measures are insufficient to mitigate the risks.


Equipment
For each update mechanism
DT.SUM-2.DN-1
Does the update mechanism ensure the software's integrity and authenticity are valid at the time of installation?
Yes
No
PASS
FAIL

Identifier	Online Firmware Update Mechanism		
Decision Node	**Decision** [E.Info.DT.SUM-2]		**Justification** [E.Just.DT.SUM-2]
DT.SUM-2.DN-1	Yes (X)	No	The update mechanism validates the integrity and authenticity of an update using a digital signature which is included in the update file (as described in E.Info.SUM-2.SUM.Sign). The update is solely installed if the signature belongs to an authorized entity at the time of installation.
Verdict	Pass		



Clause #	Title
6.x	XXX Mechanism
6.x.1	XXX-1 Applicability of mechanisms
6.x.1.1	Requirement
6.x.1.2	Rationale
6.x.1.3	Guidance
6.x.1.4	Assessment criteria
6.x.1.4.1	Assessment objective
6.x.1.4.2	Implementation categories
6.x.1.4.3	Required information
6.x.1.4.4	Conceptual assessment
6.x.1.4.5	Functional completeness assessment
6.x.1.4.6	Functional sufficiency assessment

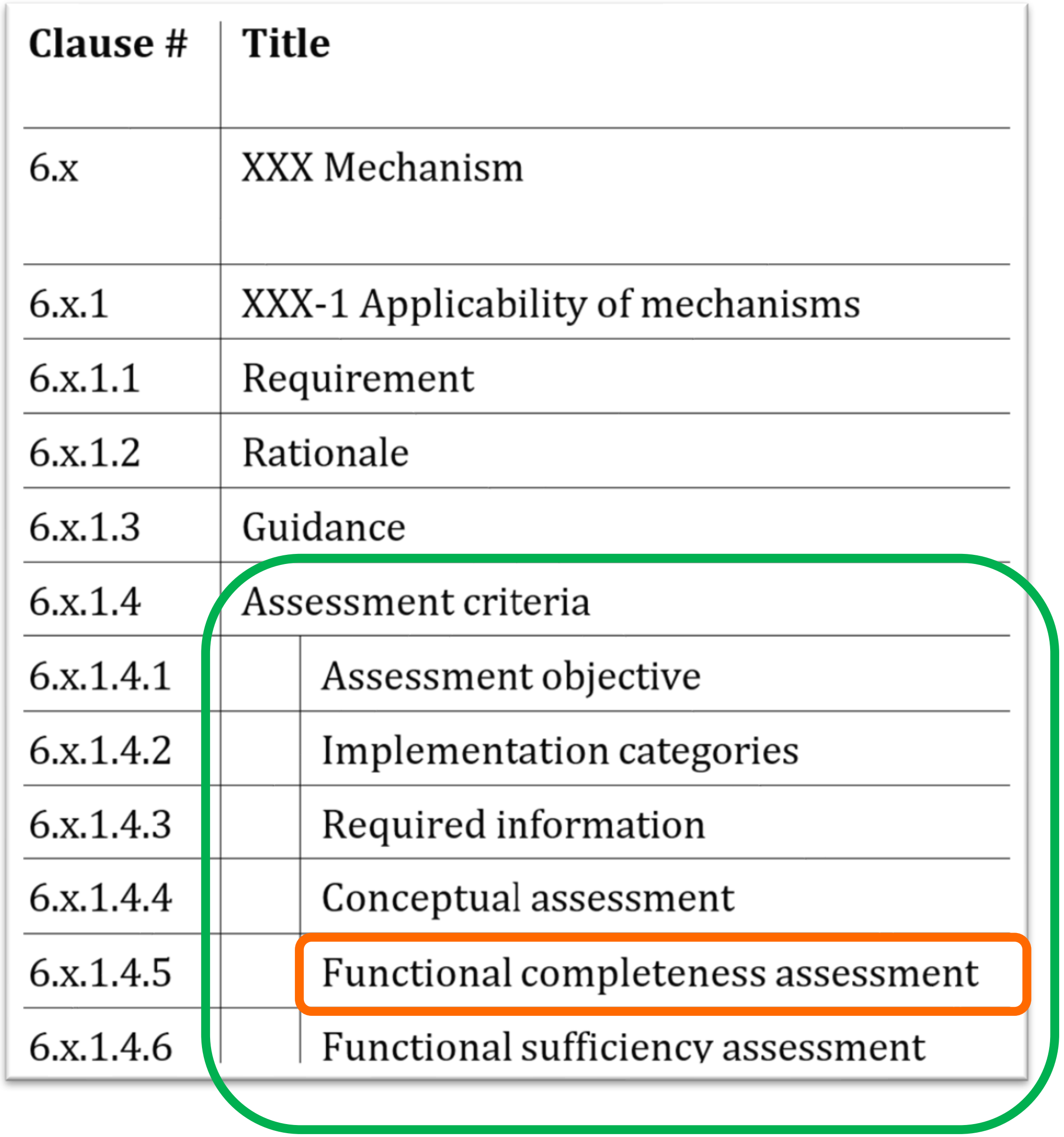
Security mechanism: Functional completeness assessment

- **Functional Completeness Assessment**

(Functional Testing)

➢ **Documentation Review: :** The evaluator carefully reviews the provided documentation. This functional completeness assessment builds upon the conceptual assessment. However, the functional assessment goes a step further by actively verifying the accuracy of the documentation through hands-on testing.

➢ **Functional Testing:** The evaluator performs hands-on testing of the equipment to confirm that its behavior matches what's described in the documentation.



Clause #	Title
6.x	XXX Mechanism
6.x.1	XXX-1 Applicability of mechanisms
6.x.1.1	Requirement
6.x.1.2	Rationale
6.x.1.3	Guidance
6.x.1.4	Assessment criteria
6.x.1.4.1	Assessment objective
6.x.1.4.2	Implementation categories
6.x.1.4.3	Required information
6.x.1.4.4	Conceptual assessment
6.x.1.4.5	Functional completeness assessment
6.x.1.4.6	Functional sufficiency assessment

ASSESSMENT

Security mechanism: Functional sufficiency assessment

- **Functional Sufficiency Assessment**

(Security Testing)

➢ **Security Testing:** This assessment combines a thorough examination of the equipment's design and functionality with active testing techniques, eg,

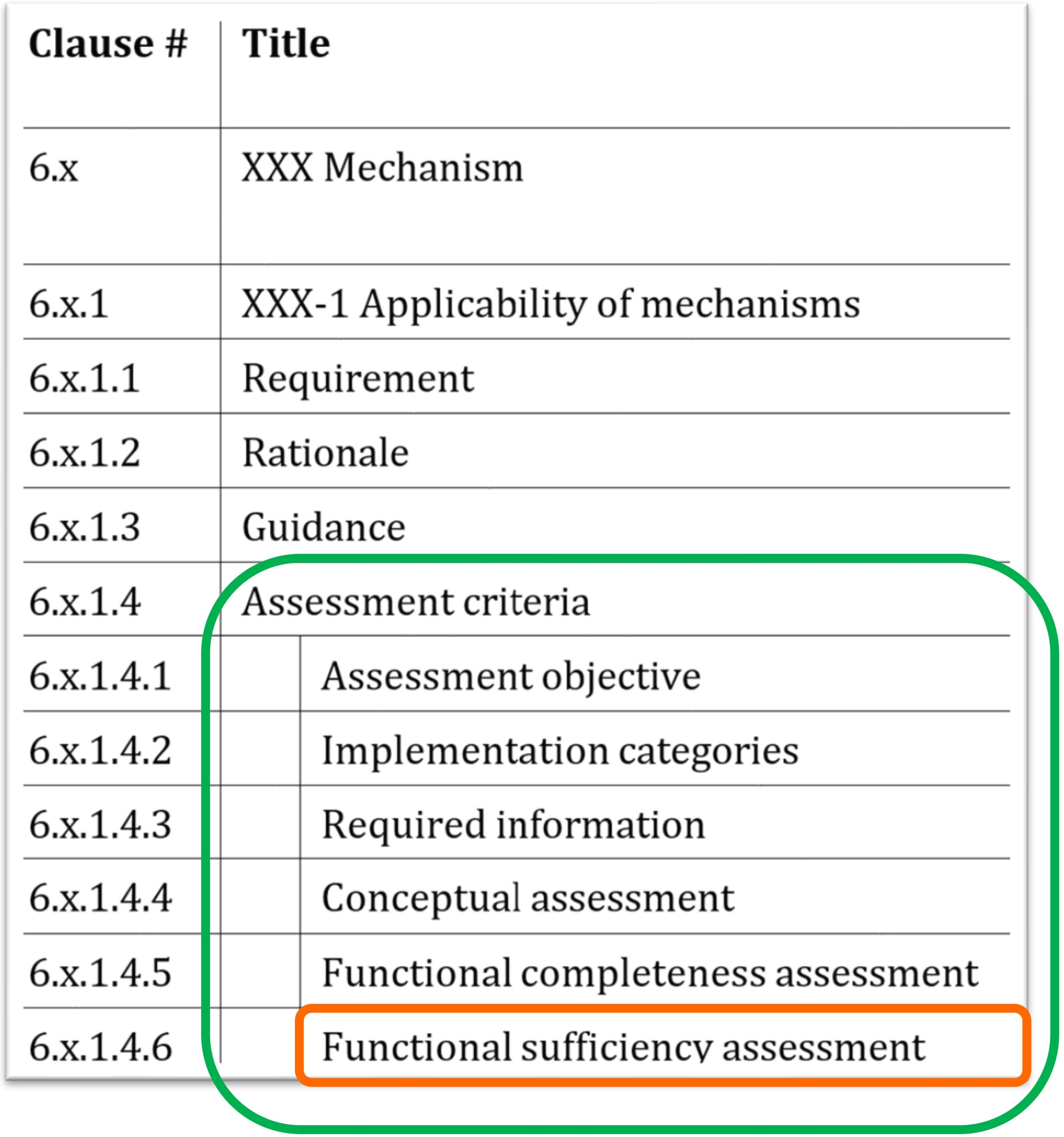
a) fuzzing on a network interface to assess its resilience against malformed input and potential buffer overflows,

b) penetration testing to simulate attacks and identify vulnerabilities,

c) code review to analyze the software implementation for security flaws,

d) stress testing to evaluate the equipment's performance under extreme conditions, and

e) other techniques tailored to a specific product type.



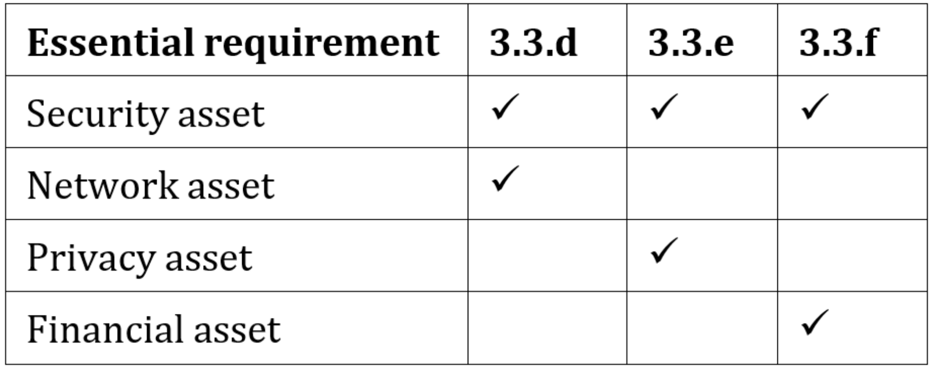
Clause #	Title
6.x	XXX Mechanism
6.x.1	XXX-1 Applicability of mechanisms
6.x.1.1	Requirement
6.x.1.2	Rationale
6.x.1.3	Guidance
6.x.1.4	Assessment criteria
6.x.1.4.1	Assessment objective
6.x.1.4.2	Implementation categories
6.x.1.4.3	Required information
6.x.1.4.4	Conceptual assessment
6.x.1.4.5	Functional completeness assessment
6.x.1.4.6	Functional sufficiency assessment

04 REQUIREMENTS

EN 18031 mandates that internet-connected radio equipment must implement essential security measures to protect network integrity, user data confidentiality, and financial transaction security. The standard also specifies requirements for hardware security.

Protected assets: Security, Network, Privacy, and Financial assets

- **Security Asset**: This encompasses any data, system, or resource that is critical for maintaining the confidentiality, integrity, and availability of information. **Security assets are subject to all three essential requirements (3.3.d, 3.3.e, and 3.3.f).**
- **Network Asset**: This category includes all the assets that make up a network infrastructure, such as configuration of servers, routers, switches, firewalls, and other network devices. **Network assets are primarily associated with requirement 3.3.d.**
- **Privacy Asset**: This refers to any information that relates to an individual's personal identity and privacy, such as names, addresses, social security numbers, health records, and financial information. **Privacy assets are primarily subject to requirement 3.3.e.**
- **Financial Asset**: This category encompasses any monetary resources or assets that have financial value, such as cash, investments, bank accounts, and financial instruments. **Financial assets are subject to requirement 3.3.f.**



Essential requirement	**3.3.d**	**3.3.e**	**3.3.f**
Security asset	✓	✓	✓
Network asset	✓		
Privacy asset		✓	
Financial asset			✓

Protected assets: Security, Network, Privacy, and Financial assets

EN 18031-1	EN 18031-2	EN 18031-3
[ACM-1] Applicability of access control mechanisms	[ACM-1] Applicability of access control mechanisms	[ACM-1] Applicability of access control mechanisms
[ACM-2] Appropriate access control mechanisms	[ACM-2] Appropriate access control mechanisms	[ACM-2] Appropriate access control mechanisms
	[ACM-3] Default access control for children in toys	
	[ACM-4] Default access control to children's privacy assets for toys and childcare equipment	
	[ACM-5] Parental/Guardian access controls for children in toys	
	[ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys	
[AUM-1] Applicability of authentication mechanisms	[AUM-1] Applicability of authentication mechanisms	[AUM-1] Applicability of authentication mechanisms
[AUM-2] Appropriate authentication mechanisms	[AUM-2] Appropriate authentication mechanisms	[AUM-2] Appropriate authentication mechanisms
[AUM-3] Authenticator validation	[AUM-3] Authenticator validation	[AUM-3] Authenticator validation
[AUM-4] Changing authenticators	[AUM-4] Changing authenticators	[AUM-4] Changing authenticators
[AUM-5] Password strength	[AUM-5] Password strength	[AUM-5] Password strength
[AUM-6] Brute force protection	[AUM-6] Brute force protection	[AUM-6] Brute force protection
[SUM-1] Applicability of update mechanisms	[SUM-1] Applicability of update mechanisms	[SUM-1] Applicability of update mechanisms
[SUM-2] Secure updates	[SUM-2] Secure updates	[SUM-2] Secure updates
[SUM-3] Automated updates	[SUM-3] Automated updates	[SUM-3] Automated updates
[SSM-1] Applicability of secure storage mechanisms	[SSM-1] Applicability of secure storage mechanisms	[SSM-1] Applicability of secure storage mechanisms
[SSM-2] Appropriate integrity protection for secure storage mechanisms	[SSM-2] Appropriate integrity protection for secure storage mechanisms	[SSM-2] Appropriate integrity protection for secure storage mechanisms
[SSM-3] Appropriate confidentiality protection for secure storage mechanisms	[SSM-3] Appropriate confidentiality protection for secure storage mechanisms	[SSM-3] Appropriate confidentiality protection for secure storage mechanisms
[SCM-1] Applicability of secure communication mechanisms	[SCM-1] Applicability of secure communication mechanisms	[SCM-1] Applicability of secure communication mechanisms
[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms	[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms	[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms
[SCM-3] Appropriate confidentiality protection for secure communication mechanisms	[SCM-3] Appropriate confidentiality protection for secure communication mechanisms	[SCM-3] Appropriate confidentiality protection for secure communication mechanisms
[SCM-4] Appropriate replay protection for secure communication mechanisms	[SCM-4] Appropriate replay protection for secure communication mechanisms	[SCM-4] Appropriate replay protection for secure communication mechanisms
[RLM-1] Applicability and appropriateness of resilience mechanisms	[LGM-1] Applicability of logging mechanisms	[LGM-1] Applicability of logging mechanisms
[NMM-1] Applicability and appropriateness of network monitoring mechanisms	[LGM-2] Persistent storage of log data	[LGM-2] Persistent storage of log data
[TCM-1] Applicability of and appropriate traffic control mechanisms	[LGM-3] Minimum number of persistently stored events	[LGM-3] Minimum number of persistently stored events
	[LGM-4] Time-related information of persistently stored dog data	[LGM-4] Time-related information of persistently stored dog data
	[DLM-1] Applicability of deletion mechanisms	
	[UNM-1] Applicability of user notification mechanisms	
	[UNM-2] Appropriate user notification content	
[CCK-1] Appropriate CCKs	[CCK-1] Appropriate CCKs	[CCK-1] Appropriate CCKs
[CCK-2] CCK generation mechanisms	[CCK-2] CCK generation mechanisms	[CCK-2] CCK generation mechanisms
[CCK-3] Preventing static default values for preinstalled CCKs	[CCK-3] Preventing static default values for preinstalled CCKs	[CCK-3] Preventing static default values for preinstalled CCKs
[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities	[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities	[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities
[GEC-2] Limit exposure of services via related network interfaces	[GEC-2] Limit exposure of services via related network interfaces	[GEC-2] Limit exposure of services via related network interfaces
[GEC-3] Configuration of optional services and the related exposed network interfaces	[GEC-3] Configuration of optional services and the related exposed network interfaces	[GEC-3] Configuration of optional services and the related exposed network interfaces
[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces	[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces	[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces
[GEC-5] No unnecessary external interfaces	[GEC-5] No unnecessary external interfaces	[GEC-5] No unnecessary external interfaces
[GEC-6] Input validation	[GEC-6] Input validation	[GEC-6] Input validation
	[GEC-7] Documentation of external sensing capabilities	
		[GEC-8] Equipment Integrity
[CRY-1] Best practice cryptography	[CRY-1] Best practice cryptography	[CRY-1] Best practice cryptography

General mechanisms on EN 18031-1

Access Control Mechanism (ACM)

The equipment shall have appropriate access control mechanisms to manage access to security/network assets and shall ensure only authorize entities have access.

Authentication Mechanism (AUM)

Authentication Mechanism shall be present for managing access to read, modify or use network function configuration or security parameters.

Secure Updates (SUM)

Secure update mechanism is present and new software can be installed with integrity and authenticity.

Secure Storage Mechanism (SSM)

Secure Storage mechanism shall be present to protect assets for confidentiality and integrity properties.

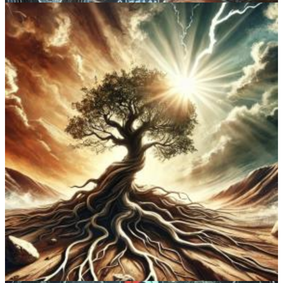
General mechanisms on EN 18031-1

Secure Communication Mechanism (SCM)

Secure Communication mechanism shall exist to protect communication of assets and be a secure mechanism to gain integrity, authenticity confidentiality and anti-replay properties.

Resilience Mechanisms (RSM)

Mitigate effects of DDoS (Denial of Service)



Network Monitoring Mechanism (NMM)

To detect attacks of DDOs.

Traffic Control Mechanism (TCM)

Mechanism to detect malicious behavior.

General mechanisms on EN 18031-1

Confidential cryptographic keys (CCK)

Verify the appropiateness of the keys, of the generation mechanisms, preventing static values of the keys

GEC: General equipment capabilities

Up-to-date software and hardware with no publicly known exploitable vulnerabilities and limit exposure services via related network interfaces as well as configuration of optional servcies, exposure of physiscal interface only when needed.

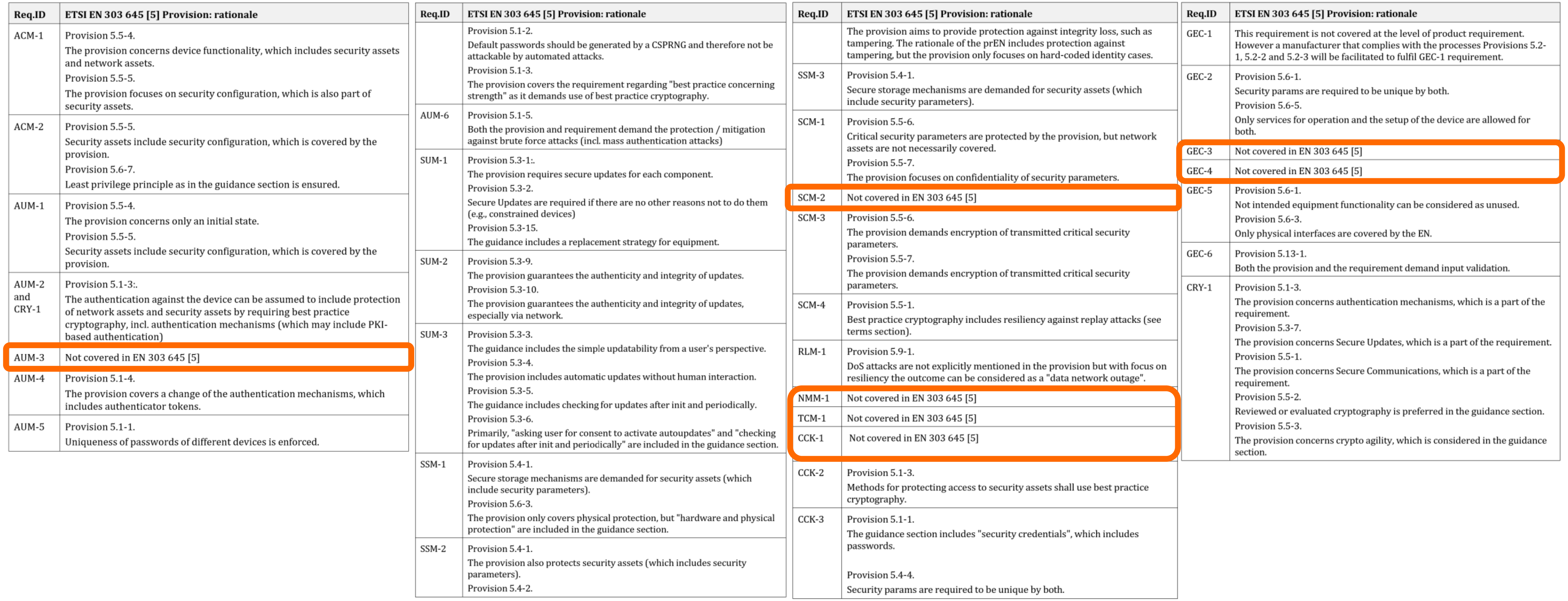
CRY: Cryptography

Best practice cryptography

05 MAPPING

EN 18031 demonstrates how complying with the security provisions of ETSI EN 303 645 can serve as a helpful framework for radio equipment manufacturers to meet the corresponding security requirements outlined in EN 18031.

Mapping with ETSI EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements): Part 1/3 (May 2024)



Req.ID	ETSI EN 303 645 [5] Provision: rationale
ACM-1	Provision 5.5-4. The provision concerns device functionality, which includes security assets and network assets. Provision 5.5-5. The provision focuses on security configuration, which is also part of security assets.
ACM-2	Provision 5.5-5. Security assets include security configuration, which is covered by the provision. Provision 5.6-7. Least privilege principle as in the guidance section is ensured.
AUM-1	Provision 5.5-4. The provision concerns only an initial state. Provision 5.5-5. Security assets include security configuration, which is covered by the provision.
AUM-2 and CRY-1	Provision 5.1-3:. The authentication against the device can be assumed to include protection of network assets and security assets by requiring best practice cryptography, incl. authentication mechanisms (which may include PKI-based authentication)
AUM-3	Not covered in EN 303 645 [5]
AUM-4	Provision 5.1-4. The provision covers a change of the authentication mechanisms, which includes authenticator tokens.
AUM-5	Provision 5.1-1. Uniqueness of passwords of different devices is enforced.
	Provision 5.1-2. Default passwords should be generated by a CSPRNG and therefore not be attackable by automated attacks. Provision 5.1-3. The provision covers the requirement regarding "best practice concerning strength" as it demands use of best practice cryptography.
AUM-6	Provision 5.1-5. Both the provision and requirement demand the protection / mitigation against brute force attacks (incl. mass authentication attacks)
SUM-1	Provision 5.3-1:. The provision requires secure updates for each component. Provision 5.3-2. Secure Updates are required if there are no other reasons not to do them (e.g., constrained devices) Provision 5.3-15. The guidance includes a replacement strategy for equipment.
SUM-2	Provision 5.3-9. The provision guarantees the authenticity and integrity of updates. Provision 5.3-10. The provision guarantees the authenticity and integrity of updates, especially via network.
SUM-3	Provision 5.3-3. The guidance includes the simple updatability from a user's perspective. Provision 5.3-4. The provision includes automatic updates without human interaction. Provision 5.3-5. The guidance includes checking for updates after init and periodically. Provision 5.3-6. Primarily, "asking user for consent to activate autoupdates" and "checking for updates after init and periodically" are included in the guidance section.
SSM-1	Provision 5.4-1. Secure storage mechanisms are demanded for security assets (which include security parameters). Provision 5.6-3. The provision only covers physical protection, but "hardware and physical protection" are included in the guidance section.
SSM-2	Provision 5.4-1. The provision also protects security assets (which includes security parameters). Provision 5.4-2.
	The provision aims to provide protection against integrity loss, such as tampering. The rationale of the prEN includes protection against tampering, but the provision only focuses on hard-coded identity cases.
SSM-3	Provision 5.4-1. Secure storage mechanisms are demanded for security assets (which include security parameters).
SCM-1	Provision 5.5-6. Critical security parameters are protected by the provision, but network assets are not necessarily covered. Provision 5.5-7. The provision focuses on confidentiality of security parameters.
SCM-2	Not covered in EN 303 645 [5]
SCM-3	Provision 5.5-6. The provision demands encryption of transmitted critical security parameters. Provision 5.5-7. The provision demands encryption of transmitted critical security parameters.
SCM-4	Provision 5.5-1. Best practice cryptography includes resiliency against replay attacks (see terms section).
RLM-1	Provision 5.9-1. DoS attacks are not explicitly mentioned in the provision but with focus on resiliency the outcome can be considered as a "data network outage".
NMM-1	Not covered in EN 303 645 [5]
TCM-1	Not covered in EN 303 645 [5]
CCK-1	Not covered in EN 303 645 [5]
CCK-2	Provision 5.1-3. Methods for protecting access to security assets shall use best practice cryptography.
CCK-3	Provision 5.1-1. The guidance section includes "security credentials", which includes passwords. Provision 5.4-4. Security params are required to be unique by both.
GEC-1	This requirement is not covered at the level of product requirement. However a manufacturer that complies with the processes Provisions 5.2-1, 5.2-2 and 5.2-3 will be facilitated to fulfil GEC-1 requirement.
GEC-2	Provision 5.6-1. Security params are required to be unique by both. Provision 5.6-5. Only services for operation and the setup of the device are allowed for both.
GEC-3	Not covered in EN 303 645 [5]
GEC-4	Not covered in EN 303 645 [5]
GEC-5	Provision 5.6-1. Not intended equipment functionality can be considered as unused. Provision 5.6-3. Only physical interfaces are covered by the EN.
GEC-6	Provision 5.13-1. Both the provision and the requirement demand input validation.
CRY-1	Provision 5.1-3. The provision concerns authentication mechanisms, which is a part of the requirement. Provision 5.3-7. The provision concerns Secure Updates, which is a part of the requirement. Provision 5.5-1. The provision concerns Secure Communications, which is a part of the requirement. Provision 5.5-2. Reviewed or evaluated cryptography is preferred in the guidance section. Provision 5.5-3. The provision concerns crypto agility, which is considered in the guidance section.

06 CONCLUSION

EN 18031 provides a comprehensive set of cybersecurity requirements aimed at mitigating the risks associated with internet-connected radio equipment, enhancing overall product security, and protecting user privacy and financial data throughout the equipment's lifecycle.

CONCLUSION | EN 18031

- Standard for radio equipment to enter EU market and comply with RED directive cybersecurity requirements. **Deadline: August, 2025.**

- Well-structured standard, work with required information to ensure streamline compliance.

- If you are a manufacturer, follow the first steps:
  - Make a **risk assessment.**
  - Prepare the **evidence** lists and structure content.
  - Check **supporting documents** such as ‘Blue guide’.

Thanks!

Applus laboratories

For any question, please contact us.
info@appluslaboratories.com

TESTING AND CERTIFICATION CENTER

www.appluslaboratories.com