CONFIRMATE

CONFormIty assessment, metRics and compliance autoMATion for the cyber resiliencE act

Penetration Testing Methodology

Output date: 2025-08-05

Status: Reviewed

Version: 0.3

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The project funded under Grant Agreement **No. 101190193** is supported by the European Cybersecurity Competence Centre. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them

List of changes

Version	Date	Description	Author(s)
0.1	21/03/25	Initial draft of the methodology shared with partners for review and feedback	Cyen
0.2	08/04/25	Revisions incorporated based on feedback received from partners	Cyen
0.3	05/08/25	Revisions incorporated based on feedback received from peers	Cyen

We sincerely thank the peer reviewers, specifically Krasen Parvanov (QRTECH), Stijn Horemans (Refracted), Ayman Khalil and Romain Muguet (Red Alert Labs), Peter Kuzmin (Kikimora), and Dominik Holzapfel (Nviso), for their critical insights and thoughtful feedback, which helped significantly enhance the accuracy and clarity of this methodology.

CRA Compliance Penetration Testing Methodology For SMEs

Contents

1. References

- Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), available here: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
- Institute for Security and Open Methodologies (ISECOM). (2010). Open Source Security Testing Methodology Manual (OSSTMM) Version 3.0, available here: https://www.isecom.org/OSSTMM.3.pdf
- Penetration Testing Execution Standard (PTES) PTES Organization. (n.d.). Penetration Testing Execution Standard (PTES), available here: https://www.pentest-standard.org/index.php/Main_Page
- Scarfone, K., & Mell, P. (2008). Technical Guide to Information Security Testing and Assessment (NIST SP 800-115), available here: https://csrc.nist.gov/pubs/sp/800/115/final
- OWASP Foundation. (n.d.). OWASP Web Security Testing Guide (WSTG), available here: https://owasp.org/www-project-web-security-testing-guide/
- MITRE Corporation. (n.d.). MITRE ATT&CK® Framework, available here: https://attack.mitre.org/
- Open Information Systems Security Group (OISSG). (2005). Information Systems Security Assessment Framework (ISSAF) Draft 0.2, available here: https://untrustednetwork.net/files/issaf0.2.1.pdf
- Threat Intelligence-Based Ethical Red Teaming (TIBER-EU) European Central Bank. (2023). TIBER-EU Framework: Threat Intelligence-Based Ethical Red Teaming, available here: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
- ETSI TS 103 701 V1.1.1 (2021-08): Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements. Available here: https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

2. Glossary: Acronyms, Terms, and Abbreviations

Acronyms

OSSTMM:	**Open Source Security Testing Methodology Manual**
OWASP:	**Open Web Application Security Project**
PTES:	**Penetration Testing Execution Standard**
NIST:	**National Institute of Standards and Technology**
SIEM:	**Security Information and Event Management**
IAM:	**Identity and Access Management (contextually inferred)**
API:	**Application Programming Interface**
VPN:	**Virtual Private Network**
SSO:	**Single Sign-On**
IoT:	**Internet of Things**
GDPR:	**General Data Protection Regulation**
ISO:	**International Organization for Standardization**
IEC:	**International Electrotechnical Commission**
CIS:	**Center for Internet Security**
CMMC:	**Cybersecurity Maturity Model Certification**
PSD2:	**Revised Payment Services Directive**
SWIFT CSP:	**Society for Worldwide Interbank Financial Telecommunication Customer Security Programme**

Terms

Penetration Testing (or pen testing):	A security exercise where a cybersecurity expert attempts to find and exploit vulnerabilities in a product and its environment, including hardware, software, interfaces, and user interaction surfaces
Vulnerability:	A weakness or flaw in a system, application, or network that can be exploited to compromise security.

Exploit:	A piece of code, technique, or process that takes advantage of a vulnerability to cause unintended behavior in a system.
Threat Actor:	An individual or group that poses a potential risk to an organization's cybersecurity could be hackers, insiders, or competitors
Risk Assessment:	The process of identifying risks that could negatively affect an organization's ability to conduct business.
Security Audit:	A systematic evaluation of the security posture of a product with digital elements, measuring its alignment with predefined technical and regulatory requirements, such as the CRA.
Incident Response Plan:	A set of instructions to help organizations detect, respond to, and recover from computer network security incidents.
Encryption:	The method by which information is converted into a secret code that hides the information's true meaning.
Manufacturer:	A natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed, or manufactured, and markets them under its name or trademark, whether for payment, monetisation, or free of charge.
Multi-factor Authentication (MFA):	An authentication method that requires the user to provide two or more verification factors to gain access to a resource, such as an application, online account, or a VPN.
Social Engineering:	The tactic of manipulating, influencing, or deceiving a victim to gain control over a computer system, or to steal personal and financial information
Tactics, Techniques, and Procedures (TTP):	Describes the behavior of a threat actor and a structured framework for executing a cyberattack.
CIA Triad (Confidentiality, Integrity, Availability):	An information security model designed to protect sensitive information from data breaches.
Product with Digital Elements (PDE):	A product that contains, or is interconnected with, software or firmware and is capable of collecting, transmitting, or processing data. PDEs include both

physical devices and software-defined products that are placed on the market or put into service.

3. Introduction

3.1 Purpose and Objectives

This document describes how to manage and conduct penetration tests against products with digital elements (PDEs) in order to support the verification of compliance with the Cyber Resilience Act (CRA)[1]. This methodology fills the practical gap by defining a CRA-aligned pentesting workflow tailored to product-level risk exposure, focusing on how such testing supports a statement of conformity. Although the CRA neither refers to nor mandates penetration testing, this remains one of the most powerful techniques for determining to what extent potential vulnerabilities are exploitable by an attacker. Consequently, a successful penetration testing exercise can strengthen the evidence base for a statement of compliance.

Throughout the development of this methodology, attention was given to a set of products identified in Annex A. These products span various levels of criticality defined in the Cyber Resilience Act (CRA). These products were selected to ensure that the methodology would be applicable and practical across different use cases, and the products serve as a silver lining across all Confirmate tools.

The approach is based on a recognised methodology (OSSTMM3[2]), which was developed in an open community and subjected to peer and cross-disciplinary review. OSSTMM3 offers a structured approach to identifying vulnerabilities and matching them with possible cyber attacks, which allows for a more accurate assessment of potential security risks.

The objectives of the proposed approach are as follows:

- To provide a structured method of penetration testing products with digital elements, whilst offering flexibility in the techniques used.
- To define a standard set of outputs that can be used to support a claim for compliance with the CRA by the manufacturer.
- To illustrate the use of the approach by explaining how it could be applied to several products taken from Important Products (Class I and Class II) and Critical products as defined by the CRA.

[1] The Cyber Resilience Act, (EU) 2024/2847: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847
[2] https://www.isecom.org/OSSTMM.3.pdf

- This methodology does not cover generic enterprise IT assessments or standalone web application pentests that do not constitute a PDE as defined by the CRA. Web-o, OWASP methodologies often cover web-only assets, which do not align with the product-centric regulatory scope required here.

3.2 Target Audience

The target audience for this document consists of the manufacturers of products with digital elements as defined by the CRA.

4. Scope

4.1 Applicability to SMEs

The approach to penetration testing proposed in this document is designed for use by Small and Medium-Sized Enterprises (SMEs). In particular, every effort has been made to keep the approach simple and easy to understand and to minimise unnecessary jargon, so that the methods proposed are within the reach of smaller companies.

This methodology is applicable to both standalone and embedded digital products within the scope of the CRA, including consumer devices, industrial controllers, smart gateways, and security-critical components. While primarily designed for pre-market and in-service testing, it may also be applied in earlier development phases to identify security weaknesses before market deployment.

4.2 Boundaries and Limitations

This document describes how to manage and execute penetration tests with the goal of supporting a claim of compliance with the requirements of the CRA. It does not cover remediation strategies, mitigation controls, or corrective security measures that may be needed following the discovery of weaknesses during testing..

Furthermore, in contrast to classical penetration tests, which target an environment, the tests covered in this document target a product. That having been said, this only makes sense if the product is housed in an appropriate environment. In this sense, the environment used to host a product throughout the tests will play a role in determining the validity of the final results. Penetration testing in this context typically takes place within a controlled laboratory setup. The testing team should either provision or approve the test bed, ensuring it reflects realistic operating conditions without weakening security assumptions.

4.3 Assumptions and Constraints

The main assumptions made in the approach presented are as follows:

- The product will be tested in a ‘laboratory environment’ as opposed to being tested in the field.

- The environment in which the product is tested will be a good approximation to the target environment (i.e., the environment in which the product will be operated).

Although example test scenarios are proposed in this approach, it is assumed that manufacturers will adapt these scenarios to reflect the nature of the product they are testing.

Constraints on the process will be identified as part of the phase 1 activities. The main constraint is that tests should be designed in such a way that they cannot have a negative impact on the operations of the testing entity.

5. Industry Standards For Testing

5.1 ETSI EN 303 645

The standard is accompanied by a test specification (TS 103 701) and implementation guide (TR 103 621)
https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf.

ETSI TS 103 701 provides structured test groups and conformance assessments tailored to consumer IoT devices. The test cases span functional, resilience, interface, and data protection requirements. In this methodology, relevant test groups from TS 103 701 are selectively applied to product categories outlined in Annex A.

ETSI EN 303 645 is the foundational European cybersecurity baseline standard for consumer Internet of Things (IoT) devices. It establishes provisions for addressing the most common and impactful attack vectors. The standard aims to ensure a minimum security baseline and acts as a reference for national regulations and conformity assessments.

5.2 OSSTMM3

An OSSTMM audit is an accurate measurement of security at an operational level that is void of assumptions and anecdotal evidence. As a methodology, it is designed to be consistent and repeatable. As an open source project, it allows for any security tester to contribute ideas for performing more accurate, actionable, and efficient security tests. Further, it allows for the free dissemination of information and intellectual property.

Compared to compliance-based standards, OSSTMM 3 focuses on real-world security validation across multiple domains, including:

- **Data Networks**: Routers, firewalls, SIEM, smart meters, and IoT devices.
- **Telecommunications**: Remote access security, VPN configurations.
- **Wireless Security**: Wi-Fi vulnerabilities, encryption standards.

It also introduced Risk Assessment Values (RAVs), which allow security teams to quantify security exposure and track vulnerabilities over time, enhancing risk management and decision-making.

5.3 OWASP Testing Guide

The OWASP Testing Guide is being developed as part of the OWASP Testing Project of the Open Web Application Security Project (OWASP). It is not a complete methodology covering a full penetration test; it is focused only on the core testing phases of web application security testing.

The guide provides a detailed discussion on the security assessment of web applications as well as their deployment stack, including web server configuration. It follows a black-box pentesting approach and is comprehensive of ‘what’ and ‘when’. There are also some guides on ‘how’, mainly in the form of listing the tools which can be used in each step or task.

5.4 PTES

The Penetration Testing Execution Standard (PTES) is the most recent penetration testing methodology to date. It was developed by a team of information security practitioners with the aim of addressing the need for a complete and up-to-date standard in penetration testing.

In addition to guiding security professionals, it also attempts to inform businesses about what they should expect from a penetration test and guide them in scoping and negotiating successful projects. It covers ‘what’ and ‘when’, but goes much deeper into the ‘how’.

The PTES is made of two main parts, which complement each other. The Pentest guidelines describe the main sections and steps of a penetration test, while the Technical guidelines discuss the specific tools and techniques to be used in each step.

5.5 NIST SP 800-15

NIST 800-115, titled "Technical Guide to Information Security Testing and Assessment," is a publication developed to provide guidelines and recommendations for conducting information security assessments to evaluate the security posture of information systems and networks.

It is aimed at assisting organizations in understanding the various types of security assessments, selecting the appropriate assessment techniques, and designing comprehensive assessment programs. The guidelines can be applied to multiple

organizations, including federal agencies, private sector organizations, and educational institutions.

Further details on popular pentesting methodologies and their comparison are available in Annex D: Methodologies Comparison. In addition, popular security guidelines and best practices are listed in Annex E.

6. Leading Methodology

The Open Source Security Testing Methodology Manual (OSSTMM 3) is the leading methodology used in this penetration testing approach. It provides a methodology for a thorough security test, herein referred to as an OSSTMM audit.

While OSSTMM 3 is the primary methodology, this penetration testing framework also integrates elements from:

- **ETSI TS 103 701 –** Relevant test cases from this conformance testing standard are incorporated into our test execution process, particularly for IoT and consumer PDEs.
- **OWASP Testing Guide** – We integrated OWASP's test cases into the reconnaissance and exploitation phases for web applications and APIs. This involves following OWASP guidelines to identify vulnerabilities such as SQL injection, cross-site scripting, and insecure session management.
- **PTES** (Penetration Testing Execution Standard) – PTES defines a structured engagement lifecycle that we integrated into the methodology. To ensure that each phase has clear objectives, output, and communication protocols, we aligned OSSTMM3 phases with PTES, resulting in a consistent and repeatable testing process.
- **NIST SP 800-115** – NIST SP 800-115 provides a solid framework for risk-based security testing. The exploitation and impact analysis phases were aligned with its guidelines to ensure systematic vulnerability identification, comprehensive risk evaluation, and detailed reporting.

7. Preparing For a Pentesting

Why test? CRA requires PDE to 'Apply effective and regular tests and reviews of the security of the product with digital elements' (Annex I, Part II, Point 3). Planning regular security assessments ensures continuous monitoring and proactive identification of vulnerabilities, maintaining resilience against emerging threats.

Who will test? In the context of CRA-aligned assessments, the choice of a penetration tester (or provider) has a direct impact on the reliability, reproducibility, and regulatory relevance of the results. SMEs could select pentesters who demonstrate the following:

- *Technical Competence*: Proven expertise in product security, embedded systems, firmware testing, and software vulnerability analysis. Providers must understand the differences between product testing and traditional enterprise environment assessments.
- *CRA Familiarity*: Demonstrable knowledge of the Cyber Resilience Act, including Annex I Part I & II requirements, and the ability to produce outputs that support CRA conformity declarations.
- *Sector-Specific Experience*: When relevant, choose providers with experience in the product's domain.
- *Legal and Ethical Assurance*: Verify that testers follow clear ethical guidelines, provide insurance coverage, and execute well-scoped legal contracts, including liability and data handling clauses.
- *Certifications and Accreditation*: Certifications such as OSCP, OSCE, CREST, or equivalent national European-level credentials are helpful. For high-risk or critical products, consider TIBER-EU or Red Team certification experience.

How long will it take? Timelines may vary based on product complexity, knowledge level (black/grey/white box), and CRA classification (default, Important, or Critical), but a generic estimate of the elapsed time for each phase could be summarised as below:

1. Preparation (5 - 10 business days, *both tester and manufacturer collaboration*), including:
    - Define scope, objectives, and testing boundaries
    - CRA Annex I requirement mapping
    - Legal agreements and stakeholder alignment
    - Client provides technical documentation

2. Testing Execution & Reporting (3 - 10 business days, *tester-led*), including:

- Intelligence gathering, exploitation, and impact analysis
- Testing of product firmware, interfaces, APIs, and security controls
- Report preparation and communication

3. Remediation (1 - 4 weeks, *manufacturer-led*)
   - Patch development, configuration fixes, internal QA
   - Optional risk acceptance and documentation updates

4. Retesting (1 - 2 business days, *both tester and manufacturer collaboration*)
   - Revalidation of resolved issues
   - Final technical confirmations and evidence gathering

8. Penetration Testing Methodology

8.1 Pre-Engagement and Planning

The first step is to define what type of test is most suitable, considering the product maturity, security risks identified for the product (internal/external), available documentation, and the possible attack vectors (how a product can be exploited). The testing could be:

- **Black-box**: Testers have no internal knowledge; simulates an external attacker.
- **Grey-box**: Testers have partial knowledge. Often led by partial access.
- **White-box**: Full internal knowledge (source code, architecture); enables deep testing.

Note that lab testing assumes partial or full knowledge (white-box).

Inputs:

- *Product identification*. For white- and grey-box testing: technical documentation would be needed, including: operational use cases, architecture diagrams, Firmware/software version, list of interfaces - internal and external (e.g., USB, BLE, APIs, web UI, ports, protocols) or any known assets/components relevant to testing, threat model (if available). Furthermore, details of previous assessments or audits (if available), including open bug tickets or unresolved test findings, could be helpful.
- Industry frameworks (e.g., OSSTMM3, PTES, NIST SP 800-115, OWASP)
- Regulatory requirements & compliance documentation, including CRA Annex I, Part I & II requirements (see Annex B: CRA Requirements)
- Points of Contact and Emergency Protocols, including a contingency procedure (what to do in case of unexpected events, such as service disruptions) during testing.
- Contractual documentation (if using external testers): Service agreements, NDAs, authorization to test, and liability waivers.

Activities:

- *Objective Definition and Scope Establishment*: This phase begins with clearly defined objectives and scopes. The focus is on ensuring that each system is tested for its unique functionalities. Scoping is critical for aligning penetration testing with the CRA's objectives and the unique attributes of the product under test. Scoping includes:
    - *Product Boundary Definition*: Define the technical perimeter (software, hardware, APIs, interfaces) of the product with digital elements (PDE).

    - *CRA Mapping*: Identify which CRA Annex I requirements apply, based on the product's risk class.
    - *Threat Modeling Input*: Incorporate known threat actors, attack surfaces, and product context.
- *Testing depth: The depth of penetration testing would correspond to the product's criticality classification under the Cyber Resilience Act (CRA).*
    - *Default and Important Class I product* testing would normally focus on externally exposed services and interfaces, access control mechanisms, data-in-transit protection, and identification of known vulnerabilities.
    - *An important Class II product* requires more thorough inspection of firmware, update mechanisms, device-to-cloud communication, authentication flows, and protocol misuse scenarios.
    - *Critical product* testing would include hardware-level security validation, such as tamper detection, fault injection resistance, and secure boot verification.
- *Legal, regulatory, and ethical considerations*: Testing is conducted with adherence to legal and regulatory requirements (e.g., privacy, data protection, IP laws) and internal policies. All required authorisations are secured, and constraints are documented so that the testing environment does not impact production operations. (see Annex B: CRA Requirements, CRA Annex I, Part I, Points 1, 2(b), 2(g), 2(j); and Annex I, Part II, Point 1.)
- *Establishment of a test lab* that mimics the operational environment of the PDE.

Outputs to subsequent phases:

- High-level methodology document
- Legal authorization forms
- Scope definition
- Engagement guidelines
- Product risk assessment report
- Stakeholder briefing

Final outputs:

- Planning & Requirements Document (D1): A detailed pentesting project plan outlining scope, roles, objectives, authorization, timing, and lab setup.
- Pre-test Risk Assessment and Stakeholder Alignment (D2): Before initiating testing, a product-specific risk assessment must be conducted to identify any potential risks that the penetration test could pose to the product's functionality, data integrity, or availability. This includes evaluating how the test could affect critical interfaces, services, and data handled by the product. Stakeholders are

briefed, and the pentesting plan must be aligned with their security requirements (incl. Annex B: CRA Requirements, CRA Annex I, Part I) and risk tolerance.

8.2 Intelligence Gathering and Reconnaissance

Inputs:

- Scope definition
- Product risk assessment report

Activities:

- Open-Source Intelligence and Asset Discovery: Open-source intelligence is used in this phase to gather as extensive information as possible. It includes mapping the digital footprint of each product and element.
- Target Profiling and Threat Landscape Analysis: An analysis for each asset is needed to determine any potential vulnerabilities. The threat landscape is also reviewed to ensure that realistic scenarios are used for the pentesting, and adversary tactics are reflected in the simulated attacks during the testing.
- Scenario Development Based on Adversary Behavior: Specific attack scenarios are formulated from the collected intelligence and data.

Outputs to subsequent phases:

- Adversary behavior scenarios and target profiles
- First version of Vulnerabilities Report (D3): Detailed findings from both external and internal assessments of the product, including risk ratings, exploitation feasibility, and remediation suggestions which provide a comprehensive view of vulnerabilities affecting the product itself.

Final outputs:

- No outputs finalised in this phase.

8.3 Testing Execution and Exploitation

Inputs:

- First version of Vulnerabilities Report (D3): Detailed findings from both external and internal assessments of the product, including risk ratings, exploitation

feasibility, and remediation suggestions which provide a comprehensive view of vulnerabilities affecting the product itself.
- Adversary behavior scenarios and target profiles
- Testing tools (e.g., Nessus, Metasploit, Wireshark). Examples of testing tools and Frameworks are listed in Annex E.
- (if available) software source code.

Activities:
- Vulnerability identification and attack simulation: Vulnerabilities are identified using techniques such as static (SAST) and dynamic application security analysis (DAST) or manual code review, where applicable. AI-driven threat intelligence may be used to enhance efficiency in vulnerability detection. Each product is tested in accordance with established standards. Vulnerability assessment activities are performed iteratively throughout the test execution and feed directly into the generation of Vulnerabilities Report D4 and serve as the primary basis for later risk evaluation. Selected test scenarios, originating from ETSI TS 103701, are listed in Annex C as they could be run as part of the pentesting that would, in addition to security, test the compliance with the CRA in alignment. Activities during this phase also validate CRA-aligned secure design and protection requirements. See Annex B: CRA Annex I, Part I, Points 2(a), 2(b), 2(d), 2(e), 2(j), 2(k); and Annex I, Part II, Point 3.
- Exploitation techniques and adversary emulation: Validating flaws by attempting to exploit them in a controlled environment. AI-assisted scanning may be used if tools are available. SMEs without such tools can rely on manual inspection or simpler automation. Examples include log anomaly detection or machine-learning-based fuzzing. Also, assessing situations in which adversaries might bypass security safeguards and gain unauthorized access.
- Post-exploitation analysis: Assessing the impact of a successful attack, including privilege escalation across the system and potential lateral movement to other users, components, or connected systems. This includes determining whether an attacker can access sensitive data, move between application modules or infrastructure segments, or compromise critical services. Functional impact details are collected by analyzing the potential consequences of each exploited vulnerability.
- Test case results are embedded in the final outputs of this phase to provide traceability of testing activities against expected behaviors.

Outputs to subsequent phases:
- Vulnerability list
- Evidence of exploitation (proof-of-concept)

- Preliminary risk ratings
- Exploitation feasibility report
- Adversary Tactics Simulation Report

Final outputs:

- Vulnerabilities Report (D3): Detailed findings from both external and internal assessments of the product, including risk ratings, exploitation feasibility, and remediation suggestions which provide a comprehensive view of vulnerabilities affecting the product itself.

8.4 Impact Analysis and Reporting

Inputs:

- Vulnerability list
- Evidence of exploitation (proof-of-concept)
- Preliminary risk ratings
- Industry-specific risk assessment standards
- Data classification policies.

Activities:

- Risk evaluation and functional impact assessment: Analyzing the severity of identified vulnerabilities, measuring their impact on CIA (Confidentiality, Integrity, or Availability). Assigning a risk rating to prioritize remediation efforts. Also, AI-based risk scoring models may be used to enhance the overall assessment phase by assigning risk levels based on real-time threat intelligence and exploitability data. This includes CRA-aligned evaluation of data integrity, resilience, and vulnerability response. See Annex B: CRA Annex I, Part I, Points 2(e), 2(f), 2(i); Annex I, Part II, Points 1, 2.
- Documentation of findings and evidence collection: Compiling in-depth reports containing vulnerability descriptions, technical evidence, and exploitation proof. Ensuring that stakeholders have a clear understanding of security gaps.
- Regulatory Compliance Flag: Translate the results from testing into regulatory compliance terms by flagging those findings linked to CRA Annex I and II requirements listed in Annex B. As such, contribute to a regulatory compliance alignment report, which can be used to justify a manufacturer's claim of conformity.

- Recommendations and actionable remediation strategies: Providing detailed guidance to mitigate identified risks. Suggesting security controls, configuration changes, and patching strategies to make the system more resilient. See Annex B: CRA Requirements

Outputs to subsequent phases:

- Risk evaluation report
- Comprehensive findings document
- Functional impact details
- Remediation recommendations
- Prioritized remediation action plan
- Regulatory compliance alignment report

Final outputs:

- Recommendations & Remediation Roadmap (D5): Prioritized recommendations with a clear remediation roadmap, including short-, medium-, and long-term actions.

8.5 Post-Engagement Follow-Up

Inputs:

- Remediation reports
- Updated system configurations and retesting results.

Activities:

- Verification of remediation efforts and retesting: Conduct retesting to validate that security flaws have been fixed. Ensuring that remediation efforts effectively eliminate vulnerabilities. Post-test activities confirm alignment with CRA expectations for security updates and disclosure. See Annex B: CRA Annex I, Part I, Points 2(h), 2(m); and Annex I, Part II, Points 2, 4, 7, 8.
- Continuous improvement and integration of lessons learned: Updating testing methodologies and security policies based on findings. AI-powered analytics help to enhance future security assessments by using lessons learned from previous tests. (see: Annex: CRA Requirements, CRA Annex I, Part I)
- Vulnerability Disclosure and Communication: Following the availability of security updates, manufacturers must prepare and publicly disclose details about resolved vulnerabilities. In cases where disclosure would introduce undue risk, the publication may be justifiably delayed until patches are widely deployed (CRA Annex I, Part II, Point 4).

Final outputs:

- Pentesting Report (D5): A typical pentesting report includes an executive summary (high-level overview, overall risk rating, test results, and priority recommendations), test scope and method (D1), activities, findings (with further details, incl. vulnerabilities (D2) and exploitation evidence), and recommendations (D4). This document could be considered a ‘review of the security of the product with digital elements’ for the purpose of CRA requirement in Annex I, Part II, Point 3 (Apply effective and regular tests and reviews of the security of the product with digital elements).

8.6 Outputs

Each engagement will produce a comprehensive set of outputs designed to address both technical and strategic needs. For any given phase of the methodology, the outputs will be one of two types: (a) outputs that are used as input to a subsequent phase and (b) outputs of the entire exercise. The outputs of the entire exercise are listed below;

- Planning & Requirements document (D1): A detailed pentesting project plan outlining objectives, scope, roles, contingency procedure, authorization, timing, and lab setup.
-
- Pre-test risk Assessment and stakeholder alignment (D2): A thorough analysis of potential risks before testing begins, ensuring alignment with stakeholders regarding scope, priorities, and objectives.
- Vulnerabilities report (D3): Detailed findings from both external and internal assessments of the product, including risk ratings, exploitation feasibility, and remediation suggestions which provide a comprehensive view of vulnerabilities affecting the product itself.
- Recommendations & remediation roadmap (D4): Prioritized recommendations with a clear remediation roadmap, including short-, medium-, and long-term actions.
- Penetration testing report (D5): A high-level overview for non-technical stakeholders summarizing key findings and strategic recommendations.

8.7 Example scenarios

The purpose of this section is to provide illustrative examples of penetration test scenarios, including approximate resource requirements and likely timing. These scenarios are only indicative in nature and could vary significantly from exercise to exercise.

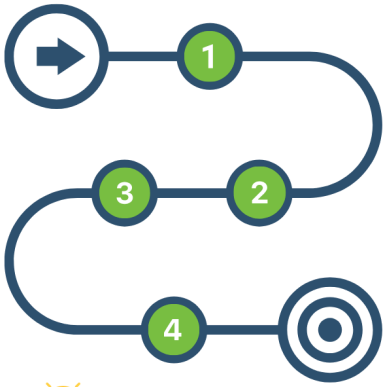
Scenario 1: Identity and Access Management (CRA's Important Product: Class I)

Testing Approach

- **Testing Type:** Grey Box (Basic credentials were provided. Pentester must enumerate internal IAM functions and privileges).
- **Complexity:** Medium (5–15 IAM functions/modules).
- **Effort Estimate:** 8–12 days of work (~15–20 days elapsed).
-

Findings & Impact

- Improper session handling exposed session tokens to unauthorized users.
- Fallback MFA logic allowed bypass using social recovery methods.
- IAM logs did not flag privilege escalation through role manipulation.



Recommendations

- Implement secure session tokens with HttpOnly, Secure and SameSite attributes.
- Enforce strict multi-factor authentication flows with no unverified fallback.
- Enable logging and alerting on privilege elevation attempts and role changes.

Attack Path

1. **Reconnaissance:** Enumerate IAM login endpoints, MFA mechanisms, and session management logic.
2. **Vulnerability Exploitation:** Bypass fallback MFA via social recovery. Hijack admin session through token harvesting.
3. **Impact Analysis & Reporting:** Identify risk of unauthorized access to admin portal and internal configurations.
4. **Follow-Up:** Patch MFA fallback logic and reconfigure session management.

CRA compliance impact

Insecure MFA fallback violates CRA Annex I, Part I, point 2(d): "Ensure protection from unauthorized access by appropriate control mechanisms."

Absence of privilege elevation logging violates CRA Annex I, Part I, point 2(l): "Provide security-related information by recording and monitoring relevant internal activity."

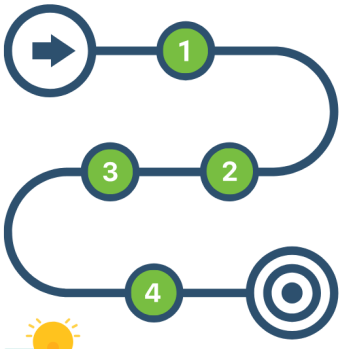
Scenario 2: Security Information and Event Management (SIEM) (CRA's Important product: Class II)

Testing Approach

- **Testing Type:** Grey Box (SIEM credentials provided; pentester simulates adversarial inputs and log tampering).
- **Complexity:** High (15–30 log sources, rule sets, and integrations).
- **Effort Estimate:** 12–15 days of work (~20–25 days elapsed).

Findings & Impact

- *SIEM failed to trigger alerts on repeated failed login attempts.*
- *Syslog injection permitted hiding of intrusion logs.*
- *Log integrity checks could be bypassed via payload evasion.*



Recommendations

- *Configure anomaly detection rules for authentication-based thresholds.*
- *Sanitize log inputs to prevent log injection.*
- *Use cryptographic log signing and validation to ensure integrity.*

Attack Path

1. **Reconnaissance:** Review SIEM ingestion points, correlation rules and alert thresholds.
2. **Vulnerability Exploitation:** Inject crafted logs to hide real attacks. Exploit lack of event correlation on failed logins.
3. **Impact Analysis & Reporting:** Evaluate how alert suppression enables persistent access.
4. **Follow-Up:** Harden parsing logic and audit rule sets.

CRA compliance impact

Log tampering without detection violates CRA Annex I, Part I, point 2(l): "Recording and monitoring relevant internal activity."

Alert bypass on repeated login failures breaches CRA Annex I, Part I, point 2(h): "Protect the availability of essential and basic functions… including mitigation against denial-of-service attacks."

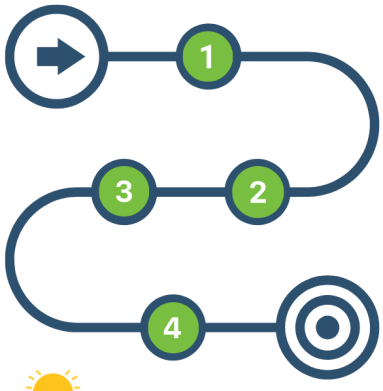
Scenario 3: Smart Meter Gateway (CRA Critical product)

Testing Approach

- **Testing Type:** Grey Box (Firmware and interface specs provided; pentester performs protocol and embedded testing).
- **Complexity:** High (Complex embedded systems and proprietary protocols).
- **Effort Estimate:** 15–20 days of work (~25–30 days elapsed).

Findings & Impact

- *Firmware update process accepted unsigned images.*
- *Secure boot validation bypassed via bootloader flaws.*
- *Replay attacks captured and resent valid encrypted communications.*



Recommendations

- *Enforce digital signature checks during firmware installation.*
- *Harden bootloader to validate cryptographic chains of trust.*
- *Include nonces and freshness checks to mitigate replay attacks.*

Attack Path

1. **Reconnaissance:** Identify firmware update endpoints and communication patterns.
2. **Vulnerability Exploitation:** Reuse captured firmware update traffic. Deploy rogue firmware.
3. **Impact Analysis & Reporting:** Demonstrate complete takeover of smart meter gateway logic.
4. **Follow-Up:** Redesign secure boot with cryptographic chain and patch replay exposure.

CRA compliance impact

Missing firmware validation violates CRA Annex I, Part I, point 2(k): "Reduce the impact of an incident using appropriate exploitation mitigation techniques."

Replay attacks exploiting firmware comms breach CRA Annex I, Part I, point 2(e): "Protect the confidentiality of stored or transmitted data by using state-of-the-art mechanisms."

Annex A: Selection of PDE considered

Important: Class I

- *Identity Management Systems*
- *Browsers*
- *Password Managers*
- *Digital Certificate Issuance Software*
- *Routers*
- *Smart home products*
- *Health-monitoring wearables*
- *SIEM systems*

Important: Class II

- *Firewalls*

Critical products

- *Smart Meter gateway*

Annex B: CRA Requirements

1. Annex I Part I – Essential Cybersecurity Requirements

CRA Requirement	CRA Requirement reference
Products with digital elements shall be designed, developed, and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks	Annex I, Part I, Point 1
(a) Be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state	Annex I, Part I, Point 2(a)
(b) Be made available on the market with a secure by default configuration, including the ability to reset to the original state.	Annex I, Part I, Point 2(b)
(c) Ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them	Annex I, Part I, Point 2(c)
(d) Ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access	Annex I, Part I, Point 2(d)

(e) Protect the confidentiality of stored, transmitted, or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms, and by using other technical means	Annex I, Part I, Point 2(e)
(f) Protect the integrity of stored, transmitted, or otherwise processed data, personal or other, commands, programs, and configuration against any manipulation or modification not authorized by the user, and report on any corruption	Annex I, Part I, Point 2(f)
(g) Process only data, personal or other, that is adequate, relevant, and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation)	Annex I, Part I, Point 2(g)
(h) Protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks	Annex I, Part I, Point 2(h)
(i) Minimise the negative impact of the products themselves or connected devices on the availability of services provided by other devices or networks	Annex I, Part I, Point 2(i)
(j) Be designed, developed, and produced to limit attack surfaces, including external interfaces	Annex I, Part I, Point 2(j)
(k) Be designed, developed, and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques	Annex I, Part I, Point 2(k)
(l) Provide security-related information by recording and monitoring relevant internal activity, including the access to or modification of data, services, or functions, with an opt-out mechanism for the user	Annex I, Part I, Point 2(l)
(m) Provide the possibility for users to securely and easily remove on a permanent basis all data and settings, and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.	Annex I, Part I, Point 2(m)

2. Annex I Part II – Vulnerability Handling Requirements

CRA Requirement	CRA Citation
Identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format, covering at the very least the top-level dependencies of the products	Annex I, Part II, Point 1
In relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates	Annex I, Part II, Point 2
Apply effective and regular tests and reviews of the security of the product with digital elements	Annex I, Part II, Point 3
Once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch	Annex I, Part II, Point 4
Put in place and enforce a policy on coordinated vulnerability disclosure	Annex I, Part II, Point 5
Take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements,	Annex I, Part II, Point 6

as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements	
Provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable, for security updates, in an automatic manner	Annex I, Part II, Point 7
Ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken	Annex I, Part II, Point 8

Annex C: Selection of ETSI TS 103701 Test Groups and Test Cases with mapping to the CRA Requirements

Test Group ID	Test case (conceptual)	Linked CRA requirement ref.
TSO 5.1: No universal default passwords	(5.1-1) The purpose of this test case is the conceptual assessment of the password-based authentication mechanisms.	Annex I, Part I, Point 2(d)
	(5.1-2) The purpose of this test case is the conceptual assessment of the generation mechanisms of pre-installed passwords.	Annex I, Part I, Point 2(d)
TSO 5.2: Implement a means to manage reports of vulnerabilities	(5.2-1) The purpose of this test case is the conceptual assessment of the publication of the vulnerability disclosure policy.	Annex I, Part II, Point 5
	(5.2-2) The purpose of this test case is the conceptual assessment of the manner in which vulnerabilities are acted on, a) and the confirmation that the preconditions for the implementation are ensured, b).	Annex I, Part II, Point 2
TSO 5.3: Keep software updated	(5.3-1) The purpose of this test case is the conceptual assessment of the updatability of software components concerning the absence of software updates, a) and the update mechanisms b).	Annex I, Part II, Point 7
	(5.3-2) The purpose of this test case is the conceptual assessment of the update installation mechanism concerning adequate measures to prevent an attacker from misusing the update installation on the DUT.	Annex I, Part II, Point 7

	(5.3-3) The purpose of this test case is the conceptual assessment of the update mechanisms concerning simplicity for the user.	Annex I, Part I, Point 2(c) Annex I, Part II, Point 8
TSO 5.4: Securely store sensitive security parameters	(5.4-1) The purpose of this test case is the conceptual assessment of the secure storage of sensitive security parameters concerning the security claims (a-c) and the completeness of the IXIT documentation d).	Annex I, Part I, Point 2(e)
	(5.4-2) The purpose of this test case is the conceptual assessment of tamper-resistant storage of hard-coded identities.	Annex I, Part I, Point 2(e)
TSO 5.5: Communicate securely	(5.5-1) The purpose of this test case is the conceptual assessment of the cryptography used for the communication mechanisms concerning the use of best practice cryptography (a-c) & the vulnerability to a feasible attack d).	Annex I, Part I, Point 2(e)
	(5.5-4) The purpose of this test case is the conceptual assessment of device functionality via a network interface in the initialized state, concerning authentication and authorization.	Annex I, Part I, Point 2(d)
TSO 5.7: Ensure software integrity	(5.7-1) The purpose of this test case is the conceptual assessment of the secure boot mechanisms of the DUT.	Annex I, Part I, Point 2(f)
	(5.7-2) The purpose of this test case is the conceptual assessment of the alerting mechanisms, a) and mechanisms for restricting the communication, b) in case of detecting an unauthorized software change.	Annex I, Part I, Point 2(f)
TSO 5.8: Ensure that personal	(5.8-1) The purpose of this test case is the conceptual assessment of the cryptography used for	Annex I, Part I, Point 2(e)

data is secure	communicating personal data between a device and a service.	
TSO 5.9: Make systems resilient to outages	(5.9-1) The purpose of this test case is the conceptual assessment of the resilience mechanisms concerning outages of the network and power.	Annex I, Part I, Point 2(h)
	(5.9-3) The purpose of this test case is the conceptual assessment of the resilience measures for the communication mechanisms.	Annex I, Part I, Point 2(h)

Annex D: Methodologies Comparison

Widely Recognised Industry Pentesting Methodologies			
Scope	**Role in this Guide**		
	Major	**Medium**	**None**
Product-specific test groups and procedures aligned with CRA Annex I.	**ETSI TS 103 701**		
Outlines baseline cybersecurity requirements for consumer IoT devices. In this methodology, it complements TS 103 701 by defining the expected secure-by-design posture that is verified through testing.	**ETSI EN 303 645**		
Provides a structured way to measure security posture using defined metrics (e.g., RAV scores). Applying OSSTMM3 metrics can support internal maturity tracking and be referenced in CRA documentation where justified.	**OSSTMM3**		
Broadly applicable to IT systems, networks, and applications. Also, it is the most detailed, with explicit phases for post-exploitation and business impact analysis.		**PTES**	
Less prescriptive about pre-/post-engagement steps, focusing on technical execution.		**NIST SP 800-115**	
Application-centric, with limited IoT-specific guidance.		**OWASP Testing Guide**	
Focuses on mapping adversary behaviors and TTPs. It does not provide a structured testing methodology but enhances attack simulations and security operations.			**MITRE ATT&CK Framework**
Focus on technical, procedural, and compliance aspects of security assessments.			**ISSAF**
Intelligence-led red teaming tailored for critical sectors, emphasizing realistic attack simulations based on emerging threats.			**TIBER-EU**

Annex E: Testing Tools and Frameworks

Category	Tools
Regulatory and Compliance Guidelines	CRA (Cyber Resilience Act), PSD2 (Revised Payment Services Directive), SWIFT CSP (Customer Security Programme)
Intelligence Gathering	recon-ng (reconnaissance framework), Maltego (data mining and link analysis), Shodan (internet scanning for connected devices), theHarvester (information gathering tool), SpiderFoot (automated OSINT gathering)
Network Security	Nmap (network scanning), Wireshark (packet analysis), Nessus (vulnerability scanning), OpenVAS (open-source vulnerability scanning)
Web and API Security	Burp Suite (web security testing), Checkmarx ZAP (automated web vulnerability scanning), Bruno (API security testing), Caido
Exploitation and Red Teaming	Metasploit (exploitation framework), BloodHound (Active Directory attack path analysis), Cobalt Strike (red teaming tool)
Cloud Security	ScoutSuite (multi-cloud security auditing), Prowler (AWS security assessment), CloudMapper (AWS architecture visualization and security checks)
Manufacturing Security	FactorySecure (manufacturing system security monitoring), OTORIO RAM2 (operational technology security platform), Claroty (industrial cybersecurity testing)
AI and Automation	Darktrace (machine learning anomaly detection), Vectra AI (AI-driven threat detection), MITRE CALDERA (automated adversary emulation), SnapAttack (automated red teaming tool)

Firmware Analysis	binwalk (firmware reverse engineering), Ghidra (software reverse engineering suite)
IoT Scanning	Shodan (device discovery and vulnerability lookup), Firmwalker (firmware configuration scanner), JTAGulator (hardware interface identification)
Hardware Interfaces	USBlyzer (USB protocol analysis), Logic Analyzers (digital signal inspection), UART/Serial tools (serial interface debugging)
Protocol Testing	Scapy (packet manipulation tool), Wireshark (protocol analysis), CAN-utils (Controller Area Network protocol testing)

Annex E: Security Guidelines and Best Practices

While Chapter 5 describes the testing standards and methodologies integrated into this penetration testing methodology, this Annex provides security best practices and implementation guidance organized by product category.

Product Category	**Relevant Standards and Guidelines**
Identity Management Systems, Browsers, Password Managers, Digital Certificate Software, SIEM Systems	OWASP ASVS Application Security Verification Standard ISO/IEC 27001 Information Security Management CIS Benchmarks Secure Configuration Guidelines ISVS Internet of Things Security Verification Standard
Consumer IoT Devices: Routers, Smart Home Devices, Health-Monitoring Wearables,	ETSI EN 303 701 Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements ISO/IEC 27400:2022, Cybersecurity. IoT security and privacy. Guidelines ENISA Good Practice Guide for Security of IoT, Secure Software Development Lifecycle GDPR (General Data Protection Regulation), ISO/IEC 27701 (Privacy Information Management), IoT Security Foundation Guidelines
Firewalls, Smart Meter Gateways	NIST SP 800-82 Guide to Industrial Control Systems Security, IEC 62443 Industrial Communication Networks – Network and System Security
Manufacturing Sector	ISA/IEC 62443 Industrial Automation and Control Systems Security ISO 9001 Quality Management Systems CMMC Cybersecurity Maturity Model Certification