iterasec

Pentesting & Security Assessment: When and How They Fit into Modern Compliance Standards

White paper

Date: 26.02.2026

Contact details: info@iterasec.com

Content Table

Introduction

For years, regulatory compliance was often viewed as a documentation exercise. If the right policies were signed and formally approved, the organization was considered compliant.

That model no longer applies.

A new wave of regulations has fundamentally shifted the focus from governance to resilience. Regulators and auditors are no longer satisfied with the existence of a vulnerability management process — they expect evidence that implemented controls withstand realistic attack scenarios.

This shift creates confusion about roles. This document addresses how offensive security assessment maps to key standards, including NIS 2, DORA, GLBA, the Cyber Resilience Act (CRA), EN 18031, FDA Medical Devices, PCI DSS, SOC 2, and ISO 27001.

Our objectives are to help you:

1. Clarify how offensive security services align with specific regulatory obligations.
2. Identify which frameworks require independent validation and which permit internal assessment.
3. Define the boundaries between "Implementation" (Internal/Consultants) and "Security Assessment" (Iterasec), so you know when you strictly need an independent partner.

At Iterasec, we specialize exclusively in the latter. We do not design compliance programs, draft policies, or deploy controls. We provide the objective, adversarial stress-tests required to prove that your security investments satisfy the rigorous demands of modern compliance.

1. The Separation of Duties: Implementation vs. Assessment

In compliance-driven environments, independence is a structural requirement. When the same team configures security controls and validates them, objectivity becomes limited. To satisfy external auditors and ensure credible results, roles must be clearly separated.

- Role A: Implementation (Internal Team / GRC Consultant)
  - Focus: Governance, Policy Writing, Remediation, System Configuration.
  - The "Build": They design the ISMS, write the risk registers, and deploy the defenses.

- Role B: Security Assessment (Iterasec)
  - Focus: Adversarial Testing, Validation, Evidence Generation.
  - The "Exam": We act as the objective third party. We do not fix the holes; we find them and prove they can be exploited.

2. The Regulatory Landscape at a Glance

Before diving into the testing requirements, it is helpful to categorize these standards by their primary objective. Most organizations fall into one or more of these "Compliance Families":

- **Family A: Operational Resilience (Keep the Business Running)**
  - Standards: **NIS 2, DORA, GLBA**.
  - Focus: Ensuring critical infrastructure and financial systems can withstand attacks and recover quickly. The regulator cares about uptime and systemic risk.

- **Family B: Product Security (Secure the Thing You Sell)**
  - Standards: **CRA, FDA Medical Devices, EN 18031.**
  - Focus: Ensuring hardware and software products are "secure by design" before they enter the market. The regulator cares about consumer safety.

- **Family C: Data Assurance (Protect the Data You Hold)**
  - Standards: **PCI DSS, SOC 2, ISO 27001.**
  - Focus: Protecting sensitive data (Credit Cards, PII, Customer Data) from theft. The auditor cares about confidentiality and access control.

3. Regulatory Cheat Sheets: Mapping Offensive Security to the Standards

Below is a detailed breakdown of the specific testing profiles for each regulation.

DORA (Digital Operational Resilience Act)

Applies to: Financial entities (Banks, Insurance, Investment Firms) and critical ICT providers.

Attribute	**Detail**
The Requirement	**Article 26:** Mandatory program of "Digital Operational Resilience Testing" (e.g., vulnerability assessments, pentesting). **Article 27:** Threat-Led Penetration Testing (TLPT) for critical entities.
Scope	Critical ICT systems, applications, and functions. For TLPT, the scope expands to "live production systems," people, and processes.
Frequency	**Standard:** Annual basic testing. **Critical Entities:** TLPT every 3 years.
Methodology	**TIBER-EU** (for TLPT) or standard industry frameworks (OWASP/NIST) for basic testing.
Iterasec Solution	**Red Teaming (TLPT) & Annual Pentesting**. Advanced simulations aligned with TIBER-EU, targeting people, processes, and technology.
External Required?	**YES (Mandatory for TLPT).** TLPT strictly requires external, qualified threat intelligence and red teaming providers. For standard testing, external is highly recommended to prove independence.

GLBA (FTC Safeguards Rule)

Applies to: Non-banking financial institutions (Auto dealers, mortgage brokers, tax preparers, payday lenders).

Attribute	Detail
The Requirement	The amended Safeguards Rule explicitly mandates annual penetration testing and semi-annual vulnerability assessments (unless 24/7 continuous monitoring is in place).
Scope	Any information system that handles, processes, or stores "Customer Information" (Non-Public Personal Information – NPI).
Frequency	**Annual** Penetration Testing. **Semi-Annual** Vulnerability Assessments.
Methodology	Standard white-box or gray-box penetration testing focusing on data exfiltration paths.
Iterasec Solution	**Annual Network & App Pentest.** A full-scope attack simulation on all systems handling customer data to satisfy the annual requirement.
External Required?	**Yes (Highly Recommended).** The "Qualified Individual" overseeing the program must report to the Board. External reports provide the necessary independence for this filing.

NIS 2 Directive

Applies to: Essential and Important entities (Energy, Transport, Health, Digital Infrastructure).

Attribute	**Detail**
The Requirement	**Article 21** mandates technical measures to manage risk, explicitly requiring entities to **assess the effectiveness** of those measures.
Scope	Critical assets, network and information systems supporting essential services.
Frequency	Regular/Periodic (Standard industry interpretation: **Annually**).
Methodology	Risk-based approach tailored to the entity's threat landscape.
Iterasec Solution	**Periodic Penetration Testing**. We provide the technical validation to prove your risk management measures are functioning effectively.
External Required?	**Recommended.** Auditors look for independent "assessments of effectiveness" to validate the internal risk reports.

CRA (Cyber Resilience Act)

Applies to: Products with digital elements (Hardware & Software) sold in the EU.

Attribute	Detail
The Requirement	Products must be "**secure by default**" and free of known vulnerabilities. **Article 13** (Obligations of Manufacturers): Mandates compliance with the essential cybersecurity requirements set out in Annex I. **Annex I, Part 1** (Product Properties): Demands products be delivered "without any known exploitable vulnerabilities" (Point 2) and designed to limit attack surfaces (Point 3h). **Annex I, Part 2** (Vulnerability Handling): Point (3) explicitly requires manufacturers to "apply effective and regular tests and reviews of the security of the product with digital elements."
Scope	**Full Ecosystem**: Device Firmware + Mobile App + Cloud API/Backend.
Frequency	**Pre-Market** (before launch) and post-market (continuous vulnerability management).
Methodology	Risk-based assessment focusing on Exploitable Vulnerabilities and Security by Design.
Iterasec Solution	**Full Ecosystem Assessment**. We test the firmware, API, and mobile app to ensure the entire product chain is secure before the Declaration of Conformity. In view of CRA, not only do you get an independent security assessment, but also a review of specific CRA-relevant security controls, processes and implementation resilience: → Factory reset, persistent memory wipe, secrets/sessions persisted → Analysing vulnerability disclosure process → BLE security → Data at rest security → Integrity controls → Attack surface analysis → SBOM and no CVE tracking

	➔ ... and more.
External Required?	**Often Mandatory**. "Critical" class products require a Notified Body (Third Party). For others, an external report acts as crucial liability protection.

FDA Medical Device Cybersecurity

Applies to: Manufacturers of medical devices (USA/Global).

Attribute	Detail
The Requirement	**Premarket Submissions (510(k))**: Guidelines mandate proof of cybersecurity testing and vulnerability management.
Scope	The medical device (software/firmware), proprietary protocols (BLE, Zigbee), and connected cloud services.
Frequency	**Pre-Market** (Submission phase) and Post-Market (Life-cycle management).
Methodology	Explicitly requires **Fuzz Testing**, static/dynamic analysis, and testing of known vulnerabilities.
Iterasec Solution	**Medical Device Pentesting**. We perform specific testing on proprietary protocols and patient safety logic.
External Required?	**Standard Practice**. FDA reviewers aggressively query self-generated reports. Independent testing provides the credibility needed for clearance.

PCI DSS v4.0

Applies to: Entities processing payment card data.

Attribute	Detail
The Requirement	**Requirement 11.3/11.4**: Penetration testing and segmentation checks. v4.0 emphasizes "Authenticated Scanning."
Scope	The entire **Cardholder Data Environment (CDE)** and any systems connected to it.
Frequency	**Annually** (Merchants/Processors). **Every 6 Months** (Service Providers).
Methodology	Must include **Segmentation Checks** (proving isolated networks are truly isolated) and Application-layer testing (OWASP Top 10).
Iterasec Solution	**PCI-Specific Pentesting**. Testing specifically for segmentation verification and application security.
External Required?	**Yes.** For most merchants/processors, external testing is the industry standard to demonstrate compliance to the QSA.

SOC 2

Applies to: Service providers (SaaS, Cloud, Managed Services) storing customer data.

Attribute	Detail
The Requirement	**Criteria CC 4.1 & CC 7.1**: Requires the entity to evaluate whether security controls (like detection and response) are present and functioning, and to actively manage vulnerabilities.
Scope	The defined "System" or "Service" (Product/Platform) and its supporting cloud infrastructure.
Frequency	**Annually** (critical for providing evidence during the Type II observation period).
Methodology	Web application and API penetration testing (e.g., OWASP ASVS) combined with cloud configuration reviews.
Iterasec Solution	**SaaS & Cloud Pentesting.** Deep-dive testing on your web application logic and cloud config to prove to the CPA firm that your product is secure against modern web attacks.
External Required?	**Standard Practice.** While not explicitly written as "external only," CPA firms rarely accept internal pentests as sufficient evidence for a SOC 2 Type II report due to the inherent conflict of interest.

ISO/IEC 27001

Applies to: Any organization establishing a formal Information Security Management System (ISMS).

Attribute	Detail
The Requirement	**Control A.8.8** (Management of technical vulnerabilities) and **Control A.8.25** (Secure Development Lifecycle) require identifying and mitigating technical flaws.
Scope	All critical assets defined within the scope of your ISMS.
Frequency	Regular/Periodic (Standard industry practice: **Annually** to satisfy surveillance and re-certification audits).
Methodology	Risk-based vulnerability assessments and network/application penetration testing.
Iterasec Solution	**Vulnerability Assessment & Pentest (VAPT)**. Provides the concrete technical evidence that your vulnerability management policy isn't just on paper, but an active, effective cycle.
External Required?	**Internal Allowed (with caveats)**. ISO allows internal testing if the testers are competent and organizationally separate from the developers. Because most companies lack this dedicated resource, utilizing an external firm is the standard approach to satisfy the external auditor.

4. Security Testing for Compliance: What the Final Report Should Contain

Every security assessment concludes with a technical report. In regulated environments, that report becomes part of the compliance evidence. A generic vulnerability summary is rarely sufficient — auditors expect documentation that clearly demonstrates scope alignment, methodology, and regulatory relevance.

Here is what defines an Iterasec Compliance Report:

- Methodology & Testing Approach: Auditors need to know how the test was conducted. We explicitly define the framework used—whether it is OWASP ASVS for web apps, TIBER-EU for DORA Red Teaming, or specific FDA guidance—ensuring the methodology aligns with the regulation.
- Executive Summary & Narrative: We provide a high-level overview of the engagement, explaining the "story" of the assessment in non-technical terms. This allows stakeholders and auditors to understand the risk posture at a glance without parsing code.
- Structured Technical Findings: Every finding is documented with precision. We include a clear description of the flaw, the technical impact, step-by-step reproduction instructions, and specific recommendations.
- Standardized Scoring (CVSS): To ensure objectivity and comparability, we strictly adhere to the Common Vulnerability Scoring System (CVSS). This provides an industry-standard severity rating that auditors accept without ambiguity.

5. Summary: Structuring Your Compliance Journey

Achieving compliance is an orchestration of three distinct layers.

1. **Planning (Internal Leadership)**: You define the scope. Are we a DORA Critical Entity? Is our product Class II or III under FDA?

2. **Implementation (Internal IT / GRC Consultants)**: You build the defenses. You write the policies, configure the encryption, and deploy the controls.

3. **Security Assessment (Iterasec)**: We validate the reality. We step in to stress-test the "Implementation" layer, providing the independent evidence required to pass the audit.

Ultimately, compliance standards are just a baseline. Iterasec operates strictly within this third layer. We provide independent penetration testing, red teaming, and adversarial validation structured around the applicable regulatory framework.

If planning and implementation are already in place, the remaining step is objective validation. That is the point at which we engage.

Our goal is to help you exceed that baseline, ensuring that your investment in compliance translates into genuine operational resilience against modern threats.