Cracking compliance. How Intigriti's PTaaS supports CREST, DORA, GDPR, and ISO

BY ELEANOR BARLOW · JUNE 16, 2025 · LAST UPDATED ON JANUARY 2, 2026

What you will learn

- **How Penetration Testing as a Service (PTaaS) helps organizations meet key cybersecurity compliance standards**, including CREST accreditation, the EU's DORA requirements, GDPR data protection obligations, and ISO/IEC 27001 information security frameworks.
- **What specific benefits compliant PTaaS delivers to security programs**, such as ongoing risk assessment, real time reporting, regulatory documentation, and strengthened operational resilience.
- **How integrating PTaaS into your security strategy can enhance trust,** reduce compliance risk, and support audit readiness across regulated industries

Penetration Testing as a Service (PTaaS) must align with core industry standards, regulations, and certifications. This is usually done to meet legal compliance, uphold industry standards, build trust, and ensure service quality for customers.

In this article, we look at how CREST, DORA, GDPR, and ISO are upheld in the context of Intigriti's PTaaS, the benefits of this, and what that means for customer experience.

CREST and Intigriti PTaaS

What is CREST?

CREST is the gold standard for quality assurance accreditation in the cybersecurity industry. It is a globally recognized not-for-profit authority that rigorously assesses organizations against stringent standards for quality, technical proficiency, and operational integrity.

'Keeping information safe in today's digital world is a serious challenge, which is why all organizations want to be sure that the cybersecurity companies they engage to test and protect their systems are reputable and competent.' – CREST.

How does CREST specifically apply to Intigriti PTaaS?

Intigriti's Penetration Testing as a Service (PTaaS) is scalable, flexible, and based on a pay-for-impact model that ensures clients only pay for validated, impactful findings. Now enhanced with CREST accreditation, Intigriti services combine trusted compliance with true innovation.

'CREST has been accrediting penetration testing companies since 2006, and by the end of 2021, it had assessed more than 300 organisations that deliver penetration testing services around the globe. During this time span, the expectations around what a penetration test is have evolved. In parallel, the toolsets,

platforms, and delivery methods that can be used to provide penetration tests have changed significantly.' – CREST.

What are the key benefits of PTaaS aligned with CREST?

CREST accreditation is a strong indicator of quality and professionalism in the cybersecurity field. Being CREST-accredited ensures that service delivery and methodology are in line with CREST standards. This means secure, reliable, and compliant solutions that not only protect customer data but also help customers maintain regulatory compliance, reduce risks, and improve their overall security posture.

Five benefits to customers include:

1. Up-to-date expertise
2. Trained security professionals
3. Customer assurance
4. Globally accepted accreditation
5. Regulatory compliance assistance

Next steps and recommendations

Read more about CREST, including benefits to bug bounty teams, and the perils of not being accredited, in '**What does it take to become CREST-accredited? Top 10 questions answered**'.

Or, read the full Intigriti and CREST news article **here**.

DORA and Intigriti PTaaS

What is DORA?

As part of the European Union's legislative framework, the Digital Operational Resilience Act (DORA) establishes a unified standard for managing operational risks related to digital information and communication technologies. These risks include cyber threats, system failures, and other digital disruptions.

'The Digital Operational Resilience Act (Regulation (EU) 2022/2554), commonly known as DORA, addresses a critical gap in EU financial regulation. Prior to DORA, financial institutions primarily managed operational risks by allocating capital to cover potential losses. This approach failed to encompass all aspects of operational resilience, particularly in relation to Information and Communication Technology (ICT).' – DORA.

Designed to support the growth of digital finance, DORA requires financial entities, such as banks, crypto-asset providers, and data reporting service providers, to implement strong and effective risk management practices. These measures aim to help organizations anticipate, mitigate, and respond to digital threats.

To enhance operational resilience, DORA mandates regular risk assessments and clear accountability structures across all financial institutions. Organizations must identify their critical ICT services along with

the associated IT systems, processes, and interdependencies. They are also required to maintain robust contingency plans to ensure continuity in the event of unexpected disruptions.

How does DORA specifically apply to Intigriti?

At Intigriti, we understand the challenges of navigating new regulations like DORA. Our platform and services are designed to help providers meet DORA's requirements while strengthening their overall cybersecurity posture.

- **Continuous security testing**: Meet DORA's Article 24(6) requirements with ongoing, real-world testing of your systems.
- **Access to elite security researchers**: Leverage the expertise of our global community of ethical hackers to uncover vulnerabilities before threat actors do.
- **Real-time vulnerability reporting:** Receive actionable insights and manage vulnerabilities in real time.
- **Comprehensive documentation**: Ensure you have the necessary evidence to demonstrate compliance to regulators.
- **Annual testing obligations:** Adopt a structured approach to meet DORA's annual testing requirements.
- **Third-party assessments:** Expand your testing scope to include critical third-party ICT service providers.

For more information on DORA, read this blog.

'The Regulation specifies that tests must use "a range of assessments, tests, methodologies, practices and tools" (Article 24(2)). Organisations must determine for themselves what to do to properly assess their defences and resilience measures, in line with the proportionality principle. One thing worth bearing in mind is your ICT supply chain. If you're a financial institution running a critical or important service in the Cloud, for example, you may need to contractually enforce (pass on) that requirement to your supplier(s).' – IT Governance.

Next steps and recommendations

To make the entire process seamless, Intigriti is committed to working with businesses to understand their environments and vulnerabilities and to navigate the growing threats and compliance processes. Speak with a security expert today.

GDPR and Intigriti PTaaS

What is GDPR?

GDPR stands for General Data Protection Regulation. While GDPR is not a legal requirement in itself, it imposes requirements for businesses when they process personal data.

'The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations

anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.' – GDPR

Read the full list of GDPR requirements here.

How does GDPR specifically apply to Intigriti PTaaS?

GDPR is not specific to PTaaS in itself. It does, however, require that all personal data must be stored and processed securely, and highlights how implementing security measures to enhance data security is paramount.

With PTaaS, companies can test, retest, assess, evaluate, and measure the effectiveness of activities in place. A lack of PTaaS may indicate to regulators that a company is not serious about its security. If a company fails to meet the requirements set up by Article 32 on 'Security of Processing', the company risks significant fines.

An example of this can be observed when the airline company, British Airways, was fined **£20m ($26m) for a data breach that impacted over 400,000 customers.**

'The final figure of £20m has come as a shock to many who were expecting it to be closer to the eye-watering £183m initially proposed, but it is still a significant moment for data privacy and GDPR. Other companies will look at the fine as a shape of things to come if they also fail to protect customers.' – BBC

What are the key benefits of Intigriti PTaaS aligned with GDPR?

With Intigriti's PTaaS, gain access to skilled and certified professionals. Every test provides a report showcasing vulnerabilities, fixes, and an attestation letter to support your measures to be GDPR compliant. Strategic guidance is provided to offer long-term security recommendations aligned with GDPR principles of data protection by design and default. Continuous PTaaS means up-to-date security and sustained GDPR compliance.

Next steps and recommendations

Intigriti's PTaaS strengthens GDPR compliance through a comprehensive, methodical approach designed to help protect personal data with precision. It offers specifically crafted testing to align with the rigorous data protection requirements of GDPR, ensuring continuous, in-depth security evaluations. Integrating Intigriti PTaaS into your GDPR compliance strategy helps your organization meet essential data protection requirements while showcasing a proactive, dedicated stance on data security. This approach not only mitigates the risk of penalties but also enhances your credibility with regulators.

ISO27001 and Intigriti PTaaS

What is ISO?

ISO stands for International Organization for Standardization. There are many standards set out by ISO, each with a different number. ISO/IEC 27001 is a standard for **Information Security Management System (ISMS)** that is recognized at an international level. It provides a framework for companies to continually

improve their information security management system and is recognized as worldwide proof of an organization's ability to align with best practices.

'ISO 27001 sets out a framework for all organizations to establish, implement, operate, monitor, review, maintain and continually improve an ISMS (information security management system).' – IT Governance

Intigriti can support, with an ISO audit. Learn more about how, here.

How does ISO specifically apply to Intigriti PTaaS?

PTaaS providers, like Intigriti, can showcase their adherence to ISO to confirm that customers' environments for testing are secure, compliant, and uphold international levels of security testing. All testing processes, handling of data, and storage of data comply with ISO controls.

"Providing the highest levels of security is at the core of what we do. It has been inherent in our own internal processes and the critical security work we do for others since our inception in 2016. ISO/IEC 27001 is the best-known and most sought-after certification by our customers. By achieving this certification, we've taken another step in ensuring our customers can have absolute confidence in the security and privacy of what we do." says Niels Hofmans, Head of Security at Intigriti. Read the full press release here.

What are the key benefits of PTaaS aligned with ISO?

Enhanced data security means secure handling of sensitive vulnerabilities and customer assets. Regulatory compliance support creates easier alignment with laws and industry standards. Process standardisation generates repeatable and efficient testing. Reduced operational risk results in reduced errors or disruptions during testing. Audit readiness forms simplify security reviews. Continuous service improvements lead to regular refinement of testing procedures. Clear expectations, SLAs, and communication mean a stronger relationship between Intigriti and the customer.

Next steps and recommendations

To learn more about Intigriti's Penetration Testing as a Service (PTaaS), visit this PTaaS page for more information.

Or, if you are uncertain about any compliance elements discussed in this article, contact the team today to learn how to work with a global pool of researchers who use different tools, perspectives, and capabilities to identify vulnerabilities your internal team might miss due to limited scope, bias, or budget.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com