bugcrowd

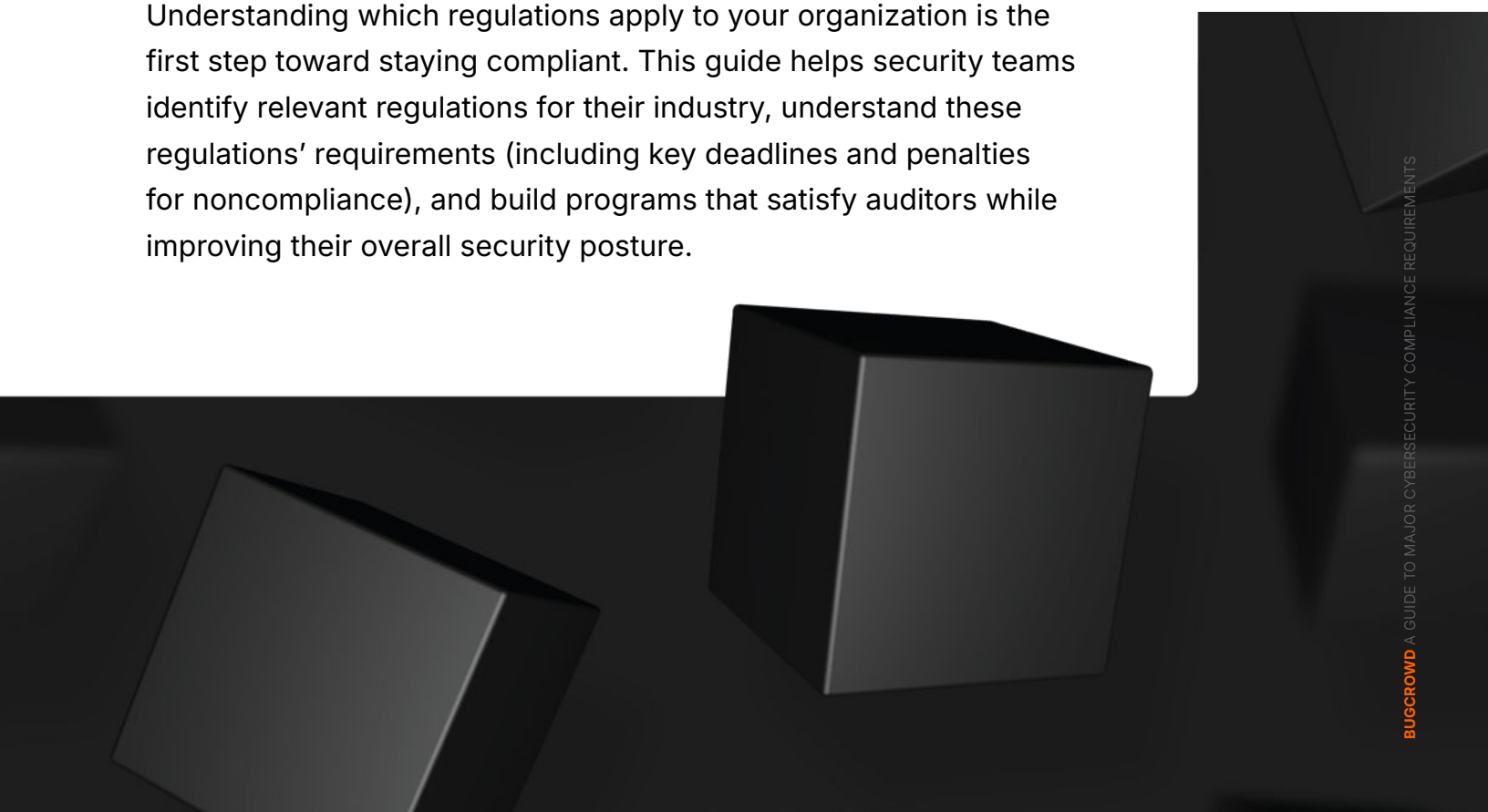
A guide to major cybersecurity compliance requirements

Table of Contents

A guide to major cybersecurity compliance requirements

Today's security teams navigate a complex web of mandatory regulations, each carrying significant **penalties for noncompliance.** To make matters more confusing, regulations overlap, change, and sometimes contradict each other, creating compliance challenges. As a result, managing **multiple overlapping regulations** with different testing requirements, reporting deadlines, and documentation standards has become the standard. For instance, a financial services company might need to comply with DORA, the GDPR, the GLBA, and PCI-DSS **simultaneously,** while a software company selling in the EU must navigate the Cyber Resilience Act, the GDPR, and NIS2.

Understanding which regulations apply to your organization is the first step toward staying compliant. This guide helps security teams identify relevant regulations for their industry, understand these regulations' requirements (including key deadlines and penalties for noncompliance), and build programs that satisfy auditors while improving their overall security posture.



Cross-industry regulations

Unlike regulations that target specific industries, such as financial services or healthcare, cross-industry regulations apply to organizations based on their geographic footprint or the types of data they process. Any company, from startups to enterprises, may be subject to these regulations if it operates in certain regions or handles specific categories of personal information.

GDPR and CCPA

General Data Protection Regulation and California Consumer Privacy Act

Effective date	✓ GDPR: May 25, 2018 ✓ CCPA: January 1, 2020
Applies to	Any organization collecting, processing, or storing the personal data of EU residents (GDPR) or California residents (CCPA)
Penalties	→ GDPR: Up to €20M or 4% of global annual revenue → CCPA: Up to $7,500 per intentional violation

The GDPR and CCPA are the two major data privacy regulations that security teams address most frequently. While the two have differences in their specific requirements for how companies should obtain privacy consent (the GDPR mandates explicit opt-in consent, while the CCPA allows opt-out mechanisms), both require organizations to implement strong data protection measures. Generally speaking, the GDPR's requirements are stricter than the CCPA's, so GDPR compliance often covers the CCPA's requirements.

These regulations require similar technical safeguards:

- ✓ Encryption of data at rest and in transit
- ✓ Access controls
- ✓ Breach notification procedures
- ✓ Comprehensive data inventory and classification programs.

Key security implications include mandatory breach notification (within 72 hours for the GDPR), data protection impact assessments for high-risk processing, and the right to erasure, which requires robust data life cycle management.

Many organizations choose to apply GDPR standards to all customers globally because it's simpler than maintaining different data-handling practices across jurisdictions and provides stronger privacy protections for everyone.

ISO 27001

Information Security Management Standard

Effective date	✓ Ongoing standard (latest version: ISO/IEC 27001:2022)
Applies to	Any organization globally seeking to demonstrate a higher level of information security management
Penalties	→ Voluntary certification

ISO 27001 provides a systematic framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). Unlike regulatory mandates, ISO 27001 is a voluntary certification that organizations pursue to demonstrate security maturity to customers, partners, and stakeholders. Many clients and business partners, especially large corporations, require their suppliers to be ISO 27001 certified, which can be achieved through an independent audit conducted by an accredited certification body.

The standard uses a risk-based approach, requiring organizations to identify information security risks and implement appropriate controls from Annex A (which contains 93 controls across 4 themes). Many controls overlap significantly with SOC 2, NIST, and other standards, so organizations can build a single compliance program rather than maintaining separate initiatives.

The primary implementation requirements include the following:

- ✓ Conducting regular risk assessments
- ✓ Establishing security policies, roles, and procedures
- ✓ Implementing technical controls (such as access management, encryption, and vulnerability management)
- ✓ Maintaining documented evidence of security practices.

SOC 2

Service Organization Control

Effective date	✓ 2010
Applies to	Technology and cloud service providers, SaaS companies, and any organization processing customer data (U.S. based but globally recognized)
Penalties	→ No regulatory penalties (voluntary)

SOC 2 has become the standard for service providers, especially SaaS companies, to demonstrate security controls to their customers and partners. The framework uses five Trust Services Criteria:

- **Security (mandatory)**—Protection against unauthorized access, including access management, logical security, and system monitoring
- **Availability**—Systems are available for operation and use as committed or agreed, with sufficient capacity and disaster recovery
- **Processing Integrity**—Transactions and data transformations are complete, accurate, timely, and authorized
- **Confidentiality**—Information is protected from unauthorized disclosure
- **Privacy**—Proper handling of personal information.

Organizations select criteria based on their services and can pursue either Type I reports (point-in-time design assessment) or Type II reports (6–12 months of operational effectiveness testing). Most enterprise customers now require SOC2 Type II compliance from their vendors.

SOC 2's flexibility means two companies with completed reports may have implemented different controls. Customers should review which criteria are covered and whether exceptions were noted, not just that a report exists. For organizations pursuing SOC 2, they must implement continuous evidence collection to demonstrate that controls are consistently operated throughout the audit period.

NIS2 Directive

Network and Information Security Directive

Effective date	✓ October 17, 2024
Applies to	Medium and large companies serving critical infrastructure sectors in the EU, regardless of the location of their headquarters, including energy, transport, banking, healthcare, and digital infrastructure
Penalties	→ Minimum of €7M or 1.4% of annual global revenue (whichever is higher)

The NIS2 Directive significantly expands the scope of the original NIS Directive, covering medium and large organizations across 18 sectors. It represents the EU's most comprehensive effort to establish baseline cybersecurity requirements across critical infrastructure.

NIS2 mandates a checklist of security capabilities that organizations must implement, including incident handling, business continuity planning, supply chain security assessments of third-party vendors and software, and vulnerability handling and disclosure. The directive explicitly requires organizations to assess cybersecurity risks across their entire supply chain, making third-party risk management a central compliance concern. The primary security requirements include implementing multi-factor authentication, encryption, continuous vulnerability assessment, security awareness training, and incident response capabilities.

Organizations must report significant incidents within 24 hours of detection and provide detailed incident reports within 72 hours. The directive also holds senior management personally accountable for cybersecurity, with potential sanctions for executives who fail to ensure compliance.

EU AI Act

Artificial Intelligence (AI) Regulation

Effective date	✓ August 1, 2024
Applies to	Organizations developing, deploying, or providing AI systems in the EU, with an emphasis on those in high-risk applications like healthcare, employment, law enforcement, and critical infrastructure
Penalties	→ Up to €35M or 7% of global annual turnover for prohibited AI → €15M or 3% for other violations → €7.5M or 1.5% for incorrect information

The EU AI Act represents the world's first comprehensive AI regulation. The Act introduced specific security requirements for AI systems, including protection against adversarial attacks, data poisoning, and model manipulation. It establishes a risk-based framework that categorizes AI systems into four tiers, from minimal risk (no restrictions) to unacceptable risk (banning the product).

If your organization deploys AI for hiring, customer service, fraud detection, or security monitoring, you may be subject to high-risk AI obligations even if you don't sell AI products. These high-risk systems must include human oversight capabilities, maintain detailed technical documentation of training data and model performance, and implement automatic logging of AI decisions. Security testing must address AI-specific threats, such as adversarial attacks, data poisoning, and model manipulation.

Financial services regulations

Financial services organizations operate under strict cybersecurity regulations that reflect the sector's importance. These regulations mandate operational resilience, third-party risk management, and continuous security testing.

DORA

Digital Operational Resilience Act

Effective date	✓ January 17, 2025
Applies to	Banks, insurance companies, investment firms, payment institutions, crypto-asset service providers, and their critical information and communications technology (ICT) third-party service providers; affects non-EU financial organizations that have offerings in the EU
Penalties	→ Up to 2% of annual global turnover or €10M for financial entities → Up to 1% or €5M for ICT service providers

DORA aims to standardize how financial entities across the EU manage ICT risks. The regulation recognizes that financial services are deeply interconnected and that a failure in one institution's technology systems can cascade across the entire sector. If you provide cloud services, software, or security solutions to EU financial entities, you're also subject to DORA compliance requirements through contractual obligations.

The regulation establishes five core pillars:

- ✓ **ICT risk management**—Establish frameworks that include governance structures, risk assessment procedures, and business continuity planning
- ✓ **Incident reporting**—Mandatory notification of major ICT incidents to regulators
- ✓ **Digital operational resilience testing**—Regular penetration testing and threat-led penetration testing (TLPT)
- ✓ **Third-party ICT risk management**—Vendor risk assessment and monitoring
- ✓ **Information sharing**—Cyber threat intelligence exchange with peers and authorities.

Beyond these contractual requirements, DORA designates certain providers as "critical" ICT third-party service providers based on their systemic importance to the financial sector. These critical providers are subject to direct regulatory oversight by EU authorities, including mandatory audits, inspections, and potential daily penalties. Regulators can also prevent critical providers from contracting with noncompliant entities.

PCI-DSS

Payment Card Industry Data Security Standard

Effective date	✓ Ongoing standard; all organizations must comply with PCI-DSS v4.0 as of March 31, 2025
Applies to	Any organization globally that stores, processes, or transmits cardholder data, such as merchants and payment processors
Penalties	→ Not directly mandated by law, but card brands can impose fines of $5,000–$100,000 per month for noncompliance; organizations may lose the ability to process card payments

PCI-DSS is a standard created by the Payment Card Industry Security Standards Council (PCI SSC), which represents major card brands like Visa, Mastercard, and American Express. PCI-DSS isn't a law. However, if organizations aren't compliant, card brands can fine or revoke an organization's ability to process payments entirely.

The standard contains 12 core requirements organized under six goals:

- ✓ Build and maintain a secure network
- ✓ Protect cardholder data
- ✓ Maintain a vulnerability management program
- ✓ Implement strong access control measures
- ✓ Regularly monitor and test networks
- ✓ Maintain an information security policy.

In practice, these requirements include multi-factor authentication for system access, encryption of cardholder data both at rest and in transit, network segmentation to reduce scope, regular vulnerability scanning and penetration testing, logging and monitoring of all access to cardholder data, and documented security policies and procedures. Organizations must also maintain current inventories of system components and conduct regular risk assessments. The standard recommends bug bounty programs as a potential solution for assessing vulnerabilities in internally developed software.

SOX

Sarbanes–Oxley Act

Effective date	✓ July 30, 2002
Applies to	All publicly traded U.S. companies, their subsidiaries, and foreign companies with U.S. listings (regardless of where they do business)
Penalties	→ Criminal penalties up to $5M and 20 years imprisonment for executives → Corporate fines up to $25M

SOX is a financial reporting regulation with significant cybersecurity implications. Section 404 of the Act requires companies to establish and maintain adequate internal controls over financial reporting—the processes, policies, and systems that ensure financial data is accurate, complete, and protected from unauthorized changes.

SOX IT compliance centers around IT General Controls (ITGCs), including access management, change management, backup procedures, and segregation of duties. These controls ensure financial data remains accurate and secure throughout its life cycle. ITGCs must protect any system handling financial data, which includes accounting applications, ERP systems, databases, and supporting infrastructure.

Companies undergo annual audits to test whether these controls were operated effectively throughout the year. Security incidents that compromise financial data integrity, like ransomware encrypting records or unauthorized access to accounting systems, create both security and compliance failures.

GLBA

Gramm–Leach–Bliley Act

Effective date	✓ November 12, 1999
Applies to	U.S. financial institutions, including banks, insurance companies, and securities firms
Penalties	→ Fines up to $100,000 per violation for institutions → Individual penalties up to $10,000 and/or 5 years imprisonment

The GLBA requires financial institutions to protect customer financial information, including credit card numbers, account numbers, income, credit history, and similar data. The Act's Safeguards Rule requires covered institutions to comply with the following:

- ✓ Designate a qualified individual to oversee their InfoSec program
- ✓ Conduct regular risk assessments
- ✓ Implement access controls and encryption
- ✓ Maintain an incident response plan
- ✓ Provide security awareness training.

Recent updates include requirements to add multi-factor authentication, encrypt data at rest and in transit, conduct regular penetration testing or vulnerability assessments, and enable continuous monitoring. Covered institutions must also deliver an annual report to their board documenting the security program's status, recent incidents, and risk assessment findings.

Software and technology regulations

CRA

Cyber Resilience Act

Effective date	✓ Started December 10, 2024 ✓ Vulnerability handling requirements: September 11, 2026 ✓ Full applicability: December 11, 2027
Applies to	Manufacturers, importers, and distributors of hardware and software products with digital elements sold in the EU, including non-EU businesses
Penalties	→ Up to €15M or 2.5% of global annual revenue (whichever is higher)

The CRA represents the EU's most ambitious attempt to regulate the cybersecurity of software and hardware products. The regulation establishes mandatory cybersecurity requirements for products "with digital elements," which covers nearly everything in modern technology, including IoT devices, network equipment, software applications, consumer electronics, and smaller components such as processors and software libraries. If your company manufactures or sells any product that connects to a network, processes data remotely, or contains software, the CRA likely applies when you sell into EU markets. Because any company selling digital products in EU markets must comply, the CRA's global impact may rival that of the GDPR's.

Manufacturers must ensure that their products are "secure by design and by default," meaning security is no longer optional. Products must ship with secure configuration settings, automatic security updates, and no known exploitable vulnerabilities. Among the many requirements, manufacturers must establish processes for receiving vulnerability reports from external researchers, promptly fix identified vulnerabilities, and report actively exploited vulnerabilities to the European Union Agency for Cybersecurity (ENISA) within 24 hours.

PSTI Act

Product Security and Telecommunications Infrastructure Act

Effective date	✓ April 29, 2024
Applies to	Manufacturers, importers, and distributors of consumer connectable products and telecommunications infrastructure in the UK
Penalties	→ Up to £20,000 per day of noncompliance → Up to £10M or 4% of global revenue for serious breaches

The UK's PSTI Act shares similar goals with the EU's CRA but focuses specifically on consumer IoT devices and telecommunications infrastructure. The Act requires manufacturers to eliminate default passwords, provide a transparent vulnerability disclosure policy, and clearly communicate the minimum period they will provide security updates. Manufacturers must establish a public point of contact for vulnerability reporting, acknowledge reports within a reasonable timeframe, and provide security updates at no additional charge to consumers.

Public sector and government contractors

NIST CSF

NIST Cybersecurity Framework

Effective date	✓ Ongoing framework (latest version: NIST CSF 2.0, February 2024)
Applies to	U.S. federal government agencies (mandated); federal contractors and critical infrastructure organizations (strongly recommended)
Penalties	→ No direct penalties but required for federal contractors → Possible contract termination or the inability to bid on federal contracts

The NIST Cybersecurity Framework, originally created in response to Executive Order 13636 to improve infrastructure security, has become the standard for federal cybersecurity (and coincidentally, also widely adopted by the private sector). Federal contractors must demonstrate alignment with NIST standards to win and maintain contracts. Many organizations use the NIST CSF as a foundation that overlaps with other requirements, such as SOC 2 and ISO 27001, to avoid duplicating their compliance work.

NIST CSF 2.0 organizes cybersecurity activities into six core functions:

- ✓ **Govern**—Establish and maintain policies, oversight, and accountability for cybersecurity risk management
- ✓ **Identify**—Understand the organization's assets, risks, and vulnerabilities
- ✓ **Protect**—Implement safeguards to prevent or limit cybersecurity incidents
- ✓ **Detect**—Monitor systems to discover security incidents
- ✓ **Respond**—Take action when incidents occur to contain and mitigate impact
- ✓ **Recover**—Restore systems and services after cybersecurity incidents.

NIST CSF 2.0 introduced significant updates to address supply chain risk management, identity and access management, and the integration of cybersecurity with enterprise risk management. The framework now explicitly addresses third-party risk, requiring organizations to understand and manage cybersecurity risks from suppliers, vendors, and business partners.

FISMA

Federal Information Security Management Act

Effective date	✓ Originally enacted in 2002; current version is FISMA Reform Act 2014
Applies to	All U.S. federal agencies and their contractors who handle federal information systems
Penalties	→ Corrective action plans and funding restrictions → Individual federal employees can face disciplinary action

FISMA establishes the framework for protecting government information, operations, and assets against threats. The law requires federal agencies to develop, document, and implement agency-wide information security programs in accordance with NIST standards and guidelines. It also applies to federal contracts, especially if contractors build, operate, or maintain federal information systems.

To comply with FISMA, agencies follow NIST's Risk Management Framework (RMF), which requires that they do the following:

- ✓ Categorize systems by risk level
- ✓ Implement appropriate security controls from NIST's catalog
- ✓ Assess the effectiveness of implemented security controls
- ✓ Obtain authorization to operate (ATO) from designated officials
- ✓ Continuously monitor security controls and threats.

Federal agencies must report FISMA compliance annually to the Office of Management and Budget and Congress. Poor performance can trigger congressional hearings and may influence funding decisions.

EO 14028

Executive Order on Improving the Nation's Cybersecurity

Effective date	✓ May 12, 2021 (with phased implementation deadlines)
Applies to	U.S. federal agencies (mandatory); software vendors and service providers selling to the federal government
Penalties	→ No direct fines, but noncompliant vendors cannot sell to the federal government

Created in response to the SolarWinds breach, Executive Order 14028 overhauled federal cybersecurity policy regarding how the government buys software and shares threat information, with requirements flowing down to contractors and vendors. EO 14028 builds upon and accelerates FISMA requirements established over 20 years ago.

The Order modernizes how the government approaches software security, responding to modern threats that weren't explicitly covered in FISMA. Federal agencies must adopt zero trust security models, implement multi-factor authentication and encryption across all systems, and deploy detailed logging and endpoint detection capabilities. The Order created standardized incident response playbooks and established the Cyber Safety Review Board to analyze significant cyber incidents. Agencies must also ensure that software vendors provide Software Bills of Materials (SBOMs), use secure development practices, and verify the integrity of software components throughout the supply chain.

Software vendors selling to federal agencies face new security requirements under EO 14028. Vendors must provide SBOMs detailing all software components and attest that their development practices follow NIST secure development guidelines. Additionally, vendors and service providers must share cyber incident and threat information with government agencies, and the Order removes contractual barriers that previously prevented or delayed this information sharing during security incidents.

BOD 20-01

CISA Binding Operational Directive on Vulnerability Disclosure

Effective date	✓ September 2, 2020
Applies to	All U.S. federal civilian agencies
Penalties	→ No direct penalties

BOD 20-01 requires federal civilian agencies to establish and maintain vulnerability disclosure programs (VDPs) that provide a clear process for security researchers to report vulnerabilities. Agencies must publish VDPs that include a clear point of contact for vulnerability reports, acknowledgment procedures, and protection for researchers acting in good faith. The directive prohibits agencies from recommending or pursuing legal action against researchers who discover and report vulnerabilities in accordance with the VDP guidelines. BOD 20-01 is part of the growing recognition that coordinating vulnerability disclosure rather than ignoring or threatening security researchers improves security outcomes.

Healthcare

HIPAA

Health Insurance Portability and Accountability Act

Effective date	✓ August 21, 1996 (with major updates in 2005 and 2013)
Applies to	U.S. healthcare providers, health plans, healthcare clearinghouses, and their business associates handling U.S. patient data
Penalties	→ Up to $50,000 per violation, with an annual maximum of $1.5M per violation category → Criminal penalties up to $250,000 and 10 years imprisonment for knowingly obtaining or disclosing personal health information (PHI)

HIPAA establishes national standards for protecting patient health information. The regulation applies to covered entities, such as healthcare providers, health plans, and clearinghouses, as well as their vendors and service providers who access PHI on their behalf.

The Security Rule, added in 2005, requires covered entities and business associates to implement administrative, physical, and technical safeguards to protect electronic PHI (ePHI). For transparency and patient protection, organizations must notify affected individuals, HHS, and the media within 60 days of an incident that affects more than 500 people.

How Bugcrowd helps with compliance

Bugcrowd's platform allows organizations of any size to address regulatory requirements at scale while reducing the burden on internal security teams. Through the platform, organizations can access a global community of vetted security researchers, workflows that scale testing efforts, and attestations that meet regulatory requirements. Here's an overview of how organizations can use Bugcrowd to meet common compliance requirements:

Transparent vulnerability handling and disclosure

Bugcrowd Vulnerability Disclosure Programs (VDPs) help organizations meet regulatory requirements for coordinated vulnerability disclosure, including those for the CRA, DORA, NIS2, PSTI, and BOD 20-01. Bugcrowd also provides a free service, VDP Compliance, to meet the basic requirements.

Continuous security monitoring

Beyond periodic compliance testing, DORA mandates continuous monitoring to detect vulnerabilities in real time. Bugcrowd offers multiple options to achieve this goal. Bugcrowd's Managed Bug Bounty and VDPs provide always-on vulnerability discovery from a global community of security researchers testing your assets 24/7. Conversely, Continuous Attack Surface Penetration Testing automatically engages pentesters when infrastructure changes are detected. The platform's triage service validates findings from all sources, prioritizes risks, and integrates remediation directly into your existing workflows.

Attack surface management and regular testing

Regulations such as DORA, PCI-DSS, and NIS2 require regular penetration testing, which Bugcrowd delivers at scale through Pen Testing as a Service (PTaaS). The platform combines this with asset discovery and risk profiling to give you visibility into your entire attack surface. Bugcrowd supports security testing of third-party systems and helps meet DORA, NIS2, and SOX requirements for vendor security validation.

Threat-led security testing

DORA and similar regulations require organizations to conduct threat-led penetration testing (TLPT) that simulates real-world attacks from sophisticated adversaries to test detection and response capabilities. Bugcrowd Red Team as a Service (RTaaS) simulates advanced persistent threats, tests blue team effectiveness, and provides comprehensive documentation of findings and remediation recommendations.

Compliance and risk reporting

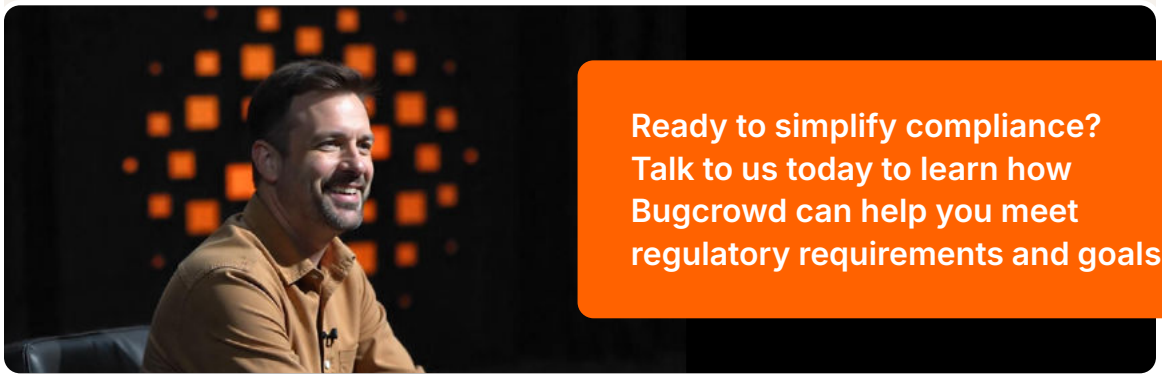
For agencies subject to BOD 20-01 and other regulations that require clear documentation, the platform automatically generates required reporting metrics. Bugcrowd's rich reporting and analytics generate on-demand reports, attestations, and executive summaries when auditors need them.

Fuzz testing

For industry regulations in which fuzzing is either mandated or recommended, Mayhem by Bugcrowd delivers continuous, advanced fuzz testing integrated with your CI workflow.

AI system security testing

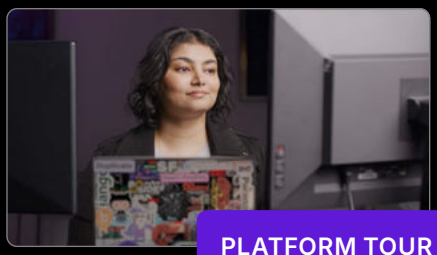
Organizations deploying high-risk AI systems under the EU AI Act are required to undergo specialized testing to validate security, fairness, and reliability. Bugcrowd offers AI-specific security assessments, including bias testing and AI penetration testing, to help organizations meet these requirements and secure their AI systems.



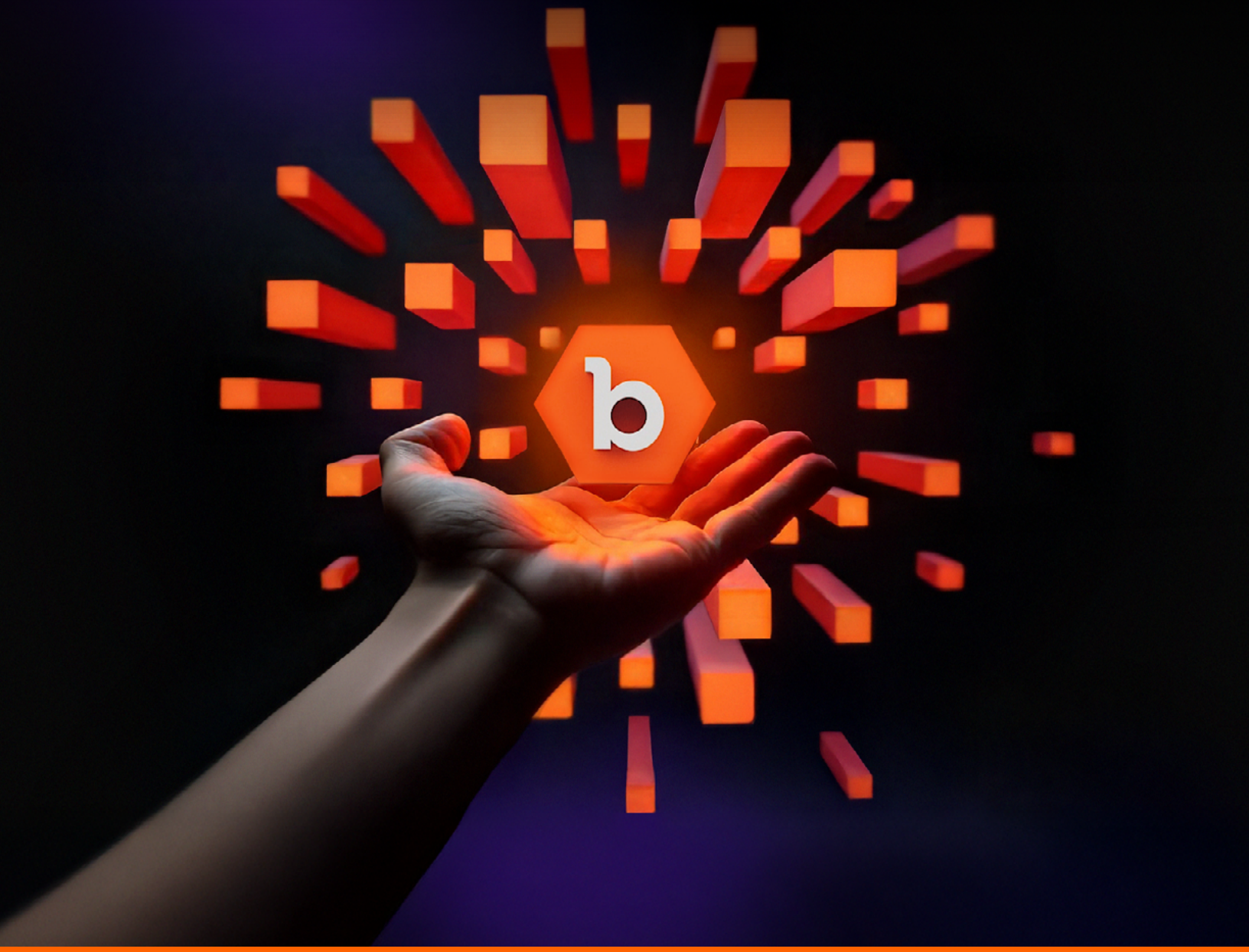
Ready to simplify compliance? Talk to us today to learn how Bugcrowd can help you meet regulatory requirements and goals.

See the Bugcrowd Platform in action

Take a 5-minute tour to get an overview of how the Bugcrowd Platform connects you with trusted hackers to help you take back control and stay ahead of attackers.



PLATFORM TOUR ▶



Unleash Human Creativity for Proactive Security

TRY BUGCROWD