DATA SHEET

ISO 27001: proving information security management resilience

ISO 27001 is a voluntary international standard that outlines a set of bestpractice guidelines for implementing an Information Security Management System (ISMS). The framework helps businesses protect the security of assets such as financial information, intellectual property, and customer data. While voluntary, ISO 27001 is popular globally, and many international organizations require partners and contractors to be certified.

Pentesting in support of the ISMS

A core component of ISO 27001 is defining an organization's risk appetite and posture and developing a plan to discover, evaluate, and handle risks. Pentesting directly supports these objectives and ensures the resilience of the ISMS.

- **Vulnerability management:** Pentesting reinforces ISO 27001's control A12.6 (Technical Vulnerability Management), which requires organizations to collect information on technical vulnerabilities in a timely fashion, use it to evaluate cyber risk, and take appropriate measures to address it.
- **Securing public networks**: Pentesting helps fulfill A14.1.2 (Securing Application Services on Public Networks), which mandates protecting services accessible via public networks from security threats.
- **Risk discovery:** Manual pentesting excels where vulnerability scanning tools fall short, identifying complex, business logic-related, and chained vulnerabilities that are critical for accurate risk evaluation.
- **Demonstrating maturity:** The framework requires organizations to demonstrate corrective actions and improvements in control maturity over time. Regular pentesting provides the evidence needed to show continuous detection and remediation guidance, thereby strengthening security controls.

By aligning pentesting efforts with ISO 27001 requirements, organizations can establish robust security programs and prove their commitment to information security for international partners.

See how Cobalt helps HeyJobs comply with ISO 27001. *Read case study >*

Book a demo to see how Cobalt can help you achieve compliance and build your offensive security program. *cobalt.io/get-started*

© 2026 Cobalt Labs, Inc. All Rights Reserved.