Privia SECURITY

# Regulation and Compliance Service

## Professional Offensive Security Services

"Take Action for a Secure and Compliant Infrastructure!"

The information contained in this document is related to the Professional Offensive Services provided by Privia Security Information and Consulting Services and is of a general nature. All information presented in this document is publicly available.

Queen Elizabeth Olympic Park, 14 East Bay Lane, Plexal, London, England, UK, E20 3BS

info@priviasecurity.co.uk

www.priviasecurity.co.uk

*“Ensuring regulatory compliance strengthens your organization’s cybersecurity posture and provides effective protection against potential threats.”*

Our regulatory and compliance penetration testing service is designed to help organizations fully align with national and international legal frameworks and industry-specific standards. In Türkiye, national regulations such as KVKK (Personal Data Protection Law), BDDK (Banking Regulation and Supervision Agency), EPDK (Energy Market Regulatory Authority), Civil Aviation Cybersecurity Directive, and the Digital Transformation Office's Information and Communication Security Guide have become mandatory requirements for enterprises.

In addition, compliance with international standards such as ISO 27001, NIST SP 800-115, and NIST SP 800-53 is critical for strengthening an organization’s information security management systems.

Privia Security supports organizations in meeting their legal obligations by proactively identifying cybersecurity vulnerabilities. Through penetration testing, existing security weaknesses are uncovered, and tailored remediation actions are recommended. These assessments not only ensure compliance with regulatory requirements but also enhance the organization’s overall maturity against cyber threats.

Penetration testing plays a vital role in protecting sensitive data, maintaining operational continuity, and avoiding potential legal penalties.

The expert team at Privia Security delivers customized solutions tailored to sector-specific needs and legal mandates, ensuring full regulatory alignment across your operations. Beyond identifying existing or potential vulnerabilities, Privia Security also develops long-term security strategies to help organizations stay prepared for evolving threats.

# Service Components

### BDDK-Compliant Penetration Testing

Penetration tests are conducted in compliance with the security standards defined by the Banking Regulation and Supervision Agency (BDDK). These tests aim to identify and remediate cybersecurity vulnerabilities within the information technology (IT) infrastructure of institutions operating in the banking and financial sectors.

BDDK-compliant penetration testing ensures the protection of customer data and financial transactions. Test results help institutions fulfill their legal obligations and avoid potential regulatory penalties.

### SPK-Compliant Penetration Testing

Penetration tests are performed in line with the regulations of the Capital Markets Board (SPK). These tests aim to detect security vulnerabilities in the systems of investment firms, brokerage houses, and portfolio management companies.

SPK-compliant penetration testing contributes to the protection of investor data and financial information. The results demonstrate regulatory compliance and provide advantages during audits.

### EPDK-Compliant Penetration Testing

Penetration tests are carried out in accordance with the standards set by the Energy Market Regulatory Authority (EPDK). These tests target the identification of security vulnerabilities in the critical infrastructures of energy production, transmission, and distribution companies.

EPDK-compliant penetration testing ensures uninterrupted and secure energy service delivery. Mitigating security vulnerabilities is vital for energy supply security and operational continuity. The tests support organizations in fulfilling their legal responsibilities.

### Civil Aviation Penetration Testing

Penetration tests are conducted in compliance with the cybersecurity directives issued by the General Directorate of Civil Aviation. These tests aim to detect vulnerabilities in the systems of airlines, airports, and other aviation industry stakeholders.

Civil aviation penetration testing is crucial for flight safety and the protection of passenger data. Test results help aviation sector organizations align with national regulations and achieve internationally recognized cybersecurity standards.

## ISO 27001-Compliant Penetration Testing

Penetration tests are conducted in accordance with the ISO/IEC 27001 Information Security Management System (ISMS) standard. These tests are critical for securing IT infrastructure and managing information security risks.

ISO 27001-compliant penetration testing is designed to effectively evaluate the organization's information security policies and controls. The results facilitate successful progress in ISO 27001 certification processes.

# FAQ

### What is a KVKK-compliant penetration test and how does it benefit businesses?

A KVKK (Personal Data Protection Law) compliant penetration test is a cybersecurity assessment conducted to ensure businesses meet the legal requirements for protecting personal data. These tests aim to identify security vulnerabilities in systems where personal data of customers and employees are stored. Penetration testing helps safeguard personal data against unauthorized access and prevents data breaches. Complying with KVKK enables businesses to avoid legal penalties and protect their reputation.

### Why are BDDK-compliant penetration tests mandatory in the financial sector?

BDDK (Banking Regulation and Supervision Agency) compliant penetration tests are mandatory for organizations in the financial sector to detect cybersecurity vulnerabilities in their IT systems. Banks and financial institutions are responsible for protecting their customers' sensitive financial data. Penetration tests carried out in accordance with BDDK regulations strengthen the organization's ability to respond to cyber threats. The information and findings obtained from these tests contribute to remediation of security weaknesses and ensuring regulatory compliance.

### What benefits do EPDK-compliant penetration tests provide in the energy sector?

EPDK (Energy Market Regulatory Authority) compliant penetration tests aim to secure the critical infrastructure of companies operating in the energy sector. These tests identify security vulnerabilities in energy production, transmission, and distribution systems, ensuring operational continuity. Cyberattacks in the energy sector can cause widespread outages, economic losses, and national security issues. EPDK-compliant tests minimize risks and enhance service quality and reliability.

### Why are SPK-compliant penetration tests important for capital markets?

SPK (Capital Markets Board) compliant penetration tests are critical for institutions operating in capital markets to maintain information security. These tests detect vulnerabilities in systems containing investor information and financial data. Adherence to SPK regulations through penetration testing prevents data breaches and ensures that investors can carry out transactions securely.

**How are penetration tests conducted under the Civil Aviation Cybersecurity Directive?**

The Civil Aviation Cybersecurity Directive includes a set of standards to ensure cybersecurity within the aviation sector. Penetration tests performed under this directive target security vulnerabilities in airline companies, airports, and air traffic control systems. These tests are crucial for maintaining uninterrupted and safe flight operations. Civil aviation penetration testing evaluates both physical and digital security measures and is categorized into Narrow Scope Penetration Tests and Broad Scope Penetration Tests.

**What advantages do ISO 27001-compliant penetration tests offer to businesses?**

ISO 27001-compliant penetration tests help businesses align their Information Security Management Systems (ISMS) with international standards. These tests assess the effectiveness of security controls necessary to protect information assets. Compliance with ISO 27001 certification increases trustworthiness among customers and business partners. Identified vulnerabilities are remediated to minimize cybersecurity risks.

**How are reports generated from regulation-compliant penetration tests utilized?**

Detailed reports are prepared for management and technical teams following regulation-compliant penetration tests. These reports provide a roadmap for mitigating identified security vulnerabilities. They include risk levels of detected weaknesses and recommended remediation measures. Businesses use these reports to develop action plans ensuring compliance with legal requirements. Additionally, the reports serve as evidence of compliance during audit processes presented to regulatory authorities. They also contribute to the development of long-term security strategies and enhance the organization’s cybersecurity maturity.

**Your Trusted Partner in Cybersecurity**

Founded in 2018 with a vision for the future of cybersecurity, Privia Security has been committed to delivering high-quality services to its clients from day one. With a strong and capable team, we provide the most reliable and comprehensive solutions across all areas of cybersecurity, ensuring our clients are well-protected in today's digital landscape.

As cyber threats continue to evolve rapidly and grow in complexity, combating them becomes increasingly challenging. At Privia Security, we offer both defensive and offensive cybersecurity strategies powered by cutting-edge technology to meet our clients' evolving needs. Through our innovative R&D products and strategic consultancy, we aim to enhance organizations' cybersecurity maturity and deliver proactive, tailored solutions. We are proud to be safeguarding the digital assets of more than 300 major organizations.

**Global and Local Cybersecurity Solutions**

Privia Security delivers cybersecurity services across a broad geographical scope, including Europe, Asia, the Middle East and the Americas. Our specialized teams in Offensive, Defensive and Forensic operations develop bespoke solutions for organizations operating in diverse sectors such as critical infrastructure, avionics systems, corporate networks and the military.

In addition, our innovative cyber warfare simulation platform, PriviaHub, offers comprehensive solutions for nations seeking to strengthen their cyber defense capabilities. PriviaHub enables the testing of cyber warfare strategies, execution of simulations and assessment of expert competencies. Designed to meet the exercise needs of private sector entities, academic institutions and military organizations, it bridges the gap between training and real-world readiness.

**A Secure Future Through Advanced Technology**

With R&D centers located in Istanbul, Ankara, London and at Cumhuriyet Technopark, we are continuously developing value-driven projects for our clients. From penetration tests and red team operations to cybersecurity training and custom enterprise solutions, we are redefining the standards in our industry. Through our slogan "Privacy For You," we bring a fresh, innovative perspective to security and privacy—ensuring that our clients' digital futures are secure.

Privia
SECURITY