Privia SECURITY

Cyber Risk Analysis Service

Professional Defensive Security Services

"Identify Risks, Establish Long-Term Strategies!"

The information contained in this document pertains to the Defensive Services performed by Privia Security Information Technology and Consultancy Services Inc. and is of a **general** nature. All information 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

“The risk identification process enables an organization to develop a long-term and sustainable security strategy against threats. Such strategies ensure security measures are properly planned and implemented.”

Cyber Risk Analysis Service is a comprehensive process designed to secure an organization’s digital or industrial assets. Its primary goal is to identify and evaluate potential security vulnerabilities threatening those assets and then to develop appropriate risk management strategies. Based on standards such as ISO 27001, NIST SP 800-30 and PCI-DSS, this analysis includes critical stages like asset inventory and valuation, threat analysis, vulnerability detection, risk assessment and risk mitigation. During the risk analysis process, an organization’s existing security controls—as well as its IT, OT and IoT infrastructures—are reviewed for effectiveness. A comprehensive action plan is then prepared to address and remediate identified vulnerabilities.

The analysis process enhances an organization’s ability to understand security weaknesses and implement suitable countermeasures. In the audits conducted for assessing existing systems, security protocols and controls are reviewed and a risk score is calculated. This risk score reflects the effectiveness of implemented security measures and highlights areas that require further improvement. The first step—penetration testing—provides a snapshot of the infrastructure’s current cybersecurity posture. Cyber Risk Analysis offers an effective solution for an organization’s security weaknesses. Data collected throughout the analysis is combined with detailed reports and recommendations, ensuring that security strategies become actionable. Reports prepared by cybersecurity experts serve as guiding documents for both management and technical teams. Risks are classified based on likelihood and impact, helping determine which countermeasures should be prioritized.

Additionally, the analysis includes detailed assessments of security components such as Security Technologies and Solutions, Network Infrastructure, Domain and Account Management. Cyber risk analysis guides organizations in continuously improving and updating their technological infrastructure. Identified security measures are aligned with existing security policies and tailored protection strategies are developed for each asset. This process helps organizations achieve their long-term security objectives and minimizes the impact of security incidents.

Service Components

Asset Inventory and Valuation

The first step in Cyber Risk Analysis Service is to create an inventory of an organization's digital or industrial assets. This process involves determining the importance of each asset in terms of business continuity and security. Identifying critical assets is fundamental to understanding which assets should be protected first. The inventory covers all assets—from physical servers to cloud services—and evaluates their exposure levels against possible attacks.

Penetration (Vulnerability) Testing

Penetration testing aims to identify potential threats to an organization's digital or industrial assets and understand the risks those threats pose. During this process, vulnerabilities exploitable by cyber attackers are discovered and the assets they could affect are analyzed. The threat analysis phase examines security weaknesses and threat sources in detail. This work helps determine the necessary measures to strengthen the organization's security infrastructure. Using specialized tools and methods, penetration testing uncovers deficiencies or errors within the current security framework.

Cybersecurity Posture Assessment

Cybersecurity Posture Assessment seeks to determine an organization's existing security level and continuously review it. This involves detailed security checks to uncover vulnerabilities and potential threats within the systems. The results are summarized as a security score, which serves as a reference for evaluating the security framework's effectiveness. Posture assessment is essential for evaluating the performance of current security controls, allowing rapid detection and remediation of vulnerabilities or technological shortcomings.

Risk Assessment and Classification

Risk assessment includes evaluating the likelihood of identified threats materializing and the potential impact of those threats. This assessment is critical for understanding how risks affect the organization's business processes. Risks are classified as Critical, High, Medium, or Low based on their probability and impact, enabling prioritization of security measures. Risk assessment also examines the alignment of security controls with the organization's strategic goals.

Cybersecurity Emergency Response Plan

A Cybersecurity Emergency Response Plan is a strategic blueprint designed to ensure an organization is prepared for urgent security incidents. The plan details the steps to be taken in response to potential security breaches and attacks. It includes emergency scenarios and follows a specific timeline, recommending necessary security controls at each stage. The plan reviews the organization's existing infrastructure, identifies areas for improvement and evaluates the effectiveness of monitoring and alert systems—implementing upgrades as needed.

Reporting

Effective cybersecurity risk management depends on continuous monitoring of the security infrastructure and periodic reporting. The monitoring process is vital for quickly detecting abnormal activities and responding to security threats in real time. Logs and analyses of security events are regularly reviewed to identify potential vulnerabilities. Reporting ensures that collected data is shared with management and security teams, prompting the implementation of remedial actions. This process creates a feedback loop to evaluate and enhance security policies and practices.

FAQ

What is Cyber Risk Analysis and why is it important?

Cyber Risk Analysis is a comprehensive process to identify, evaluate and manage potential security vulnerabilities within an organization's digital or industrial infrastructure. It helps organizations strengthen their security policies and protect sensitive data. Analyses performed in accordance with international security standards also support legal compliance.

How is Cyber Risk Analysis conducted?

Cyber Risk Analysis comprises steps such as Penetration Testing, Risk Assessment, Cybersecurity Emergency Response Planning and Reporting. First, the organization's digital assets undergo in-depth penetration testing and each asset's value is analyzed. Next, potential threats and vulnerabilities are identified and their likelihood and impact are evaluated. During the risk classification phase, the most critical risks are prioritized and appropriate security controls are recommended. An Emergency Response Plan is then developed with improvement suggestions tailored to the current infrastructure. Finally, collected data is shared with management through a detailed report.

Why is Risk Assessment important?

Risk assessment helps organizations prioritize security measures, ensuring resources are used efficiently. By classifying risks according to their probability and impact, critical vulnerabilities are addressed first. Risk assessment is fundamental for minimizing threat impacts and optimizing security policies. It also ensures the effective use of security investments and is crucial for maintaining operational continuity.

Why is Asset Inventory and Valuation performed?

Asset inventory and valuation determine the importance of an organization's digital or industrial assets. This step identifies which assets need protection and prioritization. Identifying critical assets helps direct security strategies appropriately. Valuation reveals which assets are most vulnerable to attacks, facilitating the development of tailored protection measures. By safeguarding valuable assets, organizations minimize risks such as data loss or operational disruptions.

What is a Cybersecurity Emergency Response Plan?

A Cybersecurity Emergency Response Plan is a strategic guide designed to prepare an organization for security incidents and crises. The plan outlines the steps necessary for a rapid and effective response to security breaches. It details measures and procedures to be applied under predefined scenarios to maintain business continuity and prevent data loss.

What is Cybersecurity Posture Assessment?

Cybersecurity Posture Assessment is the process of analyzing an organization's current security standing and determining its security level. It involves identifying system vulnerabilities and evaluating the effectiveness of the security framework. This assessment produces a security score, which helps organizations refine their security strategies. Findings from the assessment provide a basis for swiftly addressing and remediating identified weaknesses.

What is a Penetration Test (Vulnerability Assessment)?

A penetration test is a security evaluation that simulates attacks on an organization's digital or industrial infrastructure to uncover vulnerabilities. Cybersecurity experts attempt to exploit security flaws using techniques similar to those of real attackers. Penetration tests facilitate the swift identification and remediation of vulnerabilities. Test results offer crucial feedback for evaluating and improving security measures. These tests are also recommended after implementing new security solutions to validate infrastructure effectiveness.

How often should Cyber Risk Analysis be performed?

Cyber Risk Analysis is a continual process that should be conducted regularly based on organizational needs and industry-specific risk levels. It is recommended to repeat analyses after major infrastructure changes or following the deployment of new security controls. Performing analyses annually or biannually helps keep an organization's security posture up to date. Risk analysis is dynamic and must be continually updated to address emerging threats.

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