# Managed Security Services

Security is an inherently dynamic process. Unlike other areas of IT infrastructure, where it is possible to leave applications or data essentially unchanged for significant periods, it is impossible to take an “install it and forget it” approach to security. Vulnerabilities, threats, exploits, product bugs, patches, network configurations, application environments, and hacker tools all change constantly, making enterprise IT security a highly complex undertaking. Enterprise security is becoming ever more complex and dynamic. The complexity is caused both by business drivers and technology drivers. The number of vulnerabilities is rising fast, and the time between the announcement of vulnerabilities and their exploitation is shrinking. Many enterprise security groups are in permanent crisis mode as they struggle to cope with the complexity, especially at a time of flat budgets and compressed resources.

SSA SOFT’s Managed Security Services are a methodical approach to manage an organization’s security. The services we offer can be in house or outsourced to SSA SOFT where we will care of client network and information system security. SSA SOFT’s Managed Security Service include 24/7 monitoring and management of intrusion detection systems and firewalls, overseeing patch management and upgrades, performing security assessments and security audits, and responding to emergencies.

**Suite of Managed Security Services and IT Solutions:**

• Managed Firewall Services

• Managed Intrusion Detection Services

• Managed Virtual Private Network Service

• Managed Authentication Services

• Managed Vulnerability Protection Services

• Managed Incident Response & Forensics Services

• Managed Anti-Virus Services

• Web Application Firewall

• Network Access Control

• Bandwidth Management Solutions

• Data Leak Protection Services

• Email Protection

# Penetration Testing Services

SSA SOFT has a team of experienced consultants and Ethical Hackers to provide a complete and independent penetration testing service. We use unique techniques of penetration where our experts determines how well the organization’s current security infrastructure protect the assets by trying to gain access of the network and information assets in the same way a hacker would.

**Our Penetration testing service covers all the below services of an organization security:**  
• External Network Penetration  
• Internal Network Penetration  
• Server Application Penetration  
• Web Application Penetration  
• Mobile Application Penetration  
• Client Application Penetration  
• Physical Security Penetration

**The scope and methodology of this service include  
Black Box Testing:** In this type of testing, we don’t have any access to customer system. Customer is required to provide us their IP address range and then it is up to our technical skills to run our test. This is a classic form of penetration testing.

**White Box Testing:** In this type of testing, we would have every information and access to customers IT network and systems. We would thoroughly test the strength and effectiveness of security controls that are in place for IT infrastructure.

**Gray Box Testing:** This type of testing is hybrid of black and white testing, in which we test some of customers IT controls e.g. perimeter network and web services using black box testing technique. In addition, we apply white box testing for more extensive test of internal systems which are less prone than publically access IT systems.

# Vulnerability Assessment Services

SSA SOFT’s Vulnerability Assessment assesses the severity of weakness in IT systems or applications that can open the door to any possible attacks. Vulnerabilities can posture significant risks to both businesses’ and consumers’ systems because attacks can threaten the availability, access, or confidentiality of IT systems, applications, and the data. Our experience teams of threat experts make every effort to get you posted on every vulnerability, its exploit details, and its risk level. SSA SOFT has created a methodology for establishing vulnerability risk to ensure consistency and transparency in our processes.

Our methodology of Vulnerability assessment is based on how easy it is to exploit the vulnerability, the effect of the exploitation on your business and customers, the availability of exploit code, and other factors that impact on your business.

**Methodology and Work Scope:**

Our primary focus for the Vulnerability assessment is identifying vulnerabilities that an active hostile human threat might exploit. Although our assessment identifies both technical and non-technical weaknesses (e.g. procedural deficiencies), it is focused on an in-depth analysis of technical vulnerabilities:

• Identifying and reporting network IT infrastructure security weaknesses,

• Providing the client information about the weakness,

• Helping validate that the weakness is a vulnerability the client wants to fix,

• Assisting in identifying measures to eliminate or mitigate the vulnerability, and validating that the vulnerability is eliminated or mitigated.

# Secure Code Review

**Manual Code Review**

Many vulnerabilities cannot be discovered without looking at the code, and for many other vulnerabilities, a manual code review is simply more efficient than scanning or testing. Manual code review is the only way that several key security controls can be verified including access control, encryption, data protection, logging, and back-end system communications and usage.

Manual code review is also very useful in identifying the attack surface of an application and tracing how data flows through an application from its sources to its sinks. Manual code review helps SSA SOFT understand the actual security architecture as implemented, so that we can isolate architectural vulnerabilities.

**Static Analysis**

SSA SOFT advocates the use of code review as a part of our application assessment approach. Our use of code review makes our assessments more comprehensive and more accurate than any other approach. The use of code review also makes reviews more cost-effective.

SSA SOFT uses vulnerability scanning tools, both commercial and proprietary, as a part of our application assessment process. Vulnerability scanning is one part of our hybrid approach to application assessment. Combined with code review and security testing, our approach is more cost-effective and accurate than any other approach. We tailor scanning tools in order to get a high-quality scan, and then carefully diagnose, consolidate, and verify all of the automatically generated data.

Vulnerability scanning tools explore applications and use databases of signatures to attempt to identify weaknesses. These tools can be leveraged to find instances of XSS, CSRF, SQL Injection, unprotected directories, open ports, etc. Once the tools have been trained to understand the security controls in an application, they can be used to verify many more advanced security areas as well.

# Complete infrastructure Security Review

SSA SOFT comprehensive security assessment provides a complete understanding of your organization’s infrastructure to help you identify potential security risks and ensure compliance with security best practices. Our methodologies have been developed and proven in audits conducted with companies both large and small, ensuring our security experts have the experience to assess your organization’s exposure, provide mitigation strategies, and assist in remediation efforts.

**SSA SOFT CISR Services**

Our wide range of IT infrastructure security services including:

* Security Architecture Assessment - A comprehensive report on current security architecture posture.
* Vulnerability Scans – Detail Internal and External vulnerability scans and expert analysis.
* Device Configuration Review - Security review of device configurations and its best practices.

### **Benefits:**

* Pinpoint & correct device configuration and application issues compromising security & performance
* Classify & prioritize security architecture risks and the subsequent controls and remediation opportunities
* Identify security architecture design flaws typically discovered after a security breach
* Design & architect scalable security services that protect key information assets
* Improve security design

# ISO 27001 and ISO 22301 Consultancy Services

**ISO 27001 Consultancy Services**

Our ISO 27001 consulting services help organizations strategize, build, and certify a robust and effective Information Security Management System (ISMS). Our team of experts brings extensive experience and deep information security domain expertise (including certifications like ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, CISSP, CISA and/or CRISC) to ensure that you achieve ISO 27001 certification—on time and on budget.

Our consultants will work collaboratively with you throughout the entire certification process, from ISMS scoping through on-site Certification Audit Support. Beyond that, we provide a variety of ongoing support services to our successfully certified clients, often participating in Information Security Risk Assessments and conducting Internal ISMS Audits, among others.

**Our ISO-27001 consulting services include:**

* ISMS Scope Determination & Optimization
* Risk Assessment
* Risk Treatment Plan Development
* ISMS Gap Assessment
* Security Controls Gap Assessment
* Prioritized Roadmap Definition
* Gap Remediation Facilitation/Support
* Security Metrics
* Policy, Standards, & Procedure (PSP) Support
* ISMS Internal Audit
* Certification Audit Support

**ISO 22301 Consultancy Services**

The ISO 22301 standard for Business Continuity Management Systems (BCMS) describes the systems and processes by which a firm can best prepare for and recover from unexpected events that may impact the firm’s ability to operate.

SSA SOFT clients seeking ISO 22301 certification will receive our proven, proprietary intellectual property, which more than satisfies the ISO requirements for audit. Our consultants will then work with the firm’s leadership to customize all relevant materials to fit each client’s unique processes and infrastructure, while building teams within the client organization that are responsible for data collection and the implementation of the BCMS. Each consultant works closely with the clients to manage the evidence-collection process, ensuring that all policies or data meet auditing expectations and the standards set out in ISO 22301.