

Anitian Enterprise Security offers a comprehensive suite of security and risk assessment services for organizations of all sizes and types.

Scientific Methodology

Anitian's assessment services rely the rational, time-honored principles of the scientific method to arrive at objective and practical recommendations. Our security analysts draw conclusions from observable facts, not hype and speculation.

Pragmatic Approach to Compliance & Governance

Anitian takes a practical, pragmatic approach to compliance efforts. We respect the unique characteristics of your organization and will work to customize a compliance effort that aligns with your business and technical goals. We never force our customers into rigid, pre-defined processes.

Certified Practitioners You Can Trust

Anitian has built one of the most respected and accomplished security teams in the world. Our security analysts possess decades of experience securing and running enterprise networks. All of our consultants are certified by international bodies such as ISACA, SANS and ISC².

Auditors with Real World IT Experience

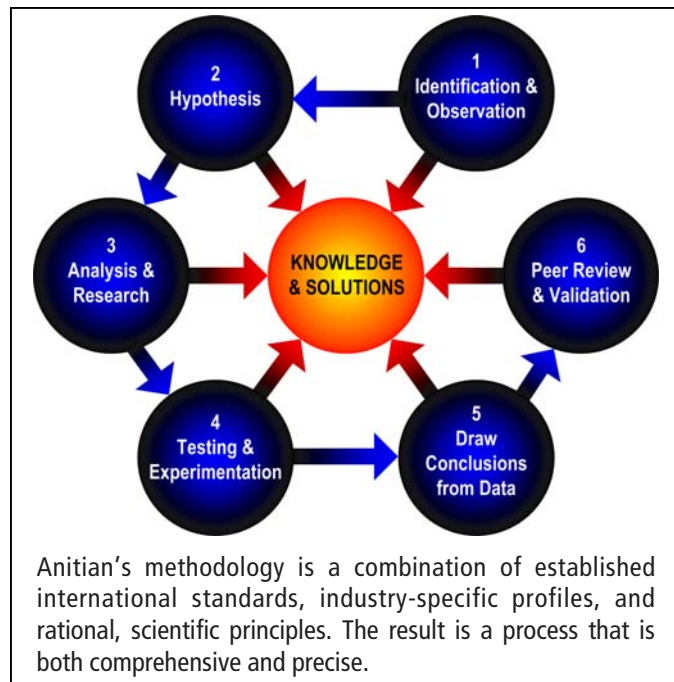
Anitian's security analysts are more than just auditors. Our team has a strong mixture of technical, business and regulatory experience. Our auditors have extensive experience deploying and managing security solutions. This provides them valuable, hands-on knowledge with the technologies and processes of compliance, making them better auditors who deliver relevant and realistic assessments.

Collaborative, Solution-Focused Consulting

Anitian uses a collaborative, constructive assessment process that avoids confrontation and division. We work closely with your internal staff to fairly analyze your information systems. Our assessment report highlights both the strengths and challenges in your environment, thereby presenting a complete, honest picture of your security posture. This allows you to properly prioritize remediation efforts.

Success That Speaks for Itself

Anitian's success speaks for itself. Our team has helped hundreds of organizations world-wide with their security and compliance needs. Our references include industry leaders who have a rigorous expectation for excellence.



The Enterprise Security Assessment Package (ESA)

Anitian's most popular assessment offering. It provides a comprehensive set of assessment and audit services all in one offering. An Anitian ESA includes:

- Network mapping & system fingerprinting
- External penetration & application testing
- Internal vulnerability scanning
- Manual confirmation of vulnerabilities
- Configuration analysis of key servers and infrastructure components
- Network architecture review
- Wireless security analysis
- Physical security review & social engineering checks
- IT policy & procedures review
- Regulatory standards gap analysis (PCI, GLBA, HIPAA, etc.)
- Organizational cultural review
- Comprehensive report with executive summary, detailed findings, recommendations and all raw data collected.

Anitian also offers a complete menu of "ala carte" risk and assessment services which are listed on the reverse of this page.

Security & Risk Assessment Services Menu

Security Assessment

- Vulnerability Scanning Analysis of systems for vulnerabilities or weaknesses.
- Penetration Testing Focused testing of systems for resistance to attack.
- Application Testing Test applications for vulnerabilities such as SQL injection, input fuzzing & privilege escalation.
- Code Review Inspect source code of applications for security & integrity risks.
- Vulnerability Scanning Automated scanning of internal and/or external systems with human analysis and reporting.
- Validation Testing Validate the existence and effectiveness of safeguards implemented since last assessment.

Compliance Assessment & IT Auditing

- Payment Card (PCI) Anitian is a Qualified Security Assessor (QSA) and uses an Approved Scanning Vendor (ASV) for all PCI compliance projects.
- Financial Services Compliance assessment for GLBA, FFIEC or NCUA standards.
- Energy / Utilities Analyze organization against NERC CIP standards and best practices associated to SCADA systems.
- Service Industry Review policies, procedures and systems for compliance with the SAS-70 standards.
- Healthcare Analyze and audit organization against the HIPAA regulations and healthcare best practices.
- Government Determine compliance with FISMA, DIACAP or other federal, state and local regulations.

Security Policies & Risk Assessment

- Risk Assessment Develop risk profiles for the IT environment, systems or applications.
- Policy Review & Development Design and document organizational policies, procedures & standards.
- Advisory Reports Strategic reports to advise an organization on security practices.
- Disaster Recovery & Business Continuity Develop practices and procedures for data backup, storage and recovery as well as business continuity operations.
- Gap Analysis Compare current security and operational status to established standards.
- Awareness Training Educate staff on security procedures, practices and policies.

Technology Validation & Analysis

- Security Validation Validate the effectiveness of existing safeguards and controls.
- Configuration Analysis Analyze and test the configuration of safeguards such as firewalls, intrusion prevention, VPN, etc.
- Identity Management Review the configuration, management and use of identity repositories such as Active Directory.
- Wireless Security Analyze wireless technologies and security options.
- Mobile Devices Evaluate the effectiveness of safeguards for PDAs, laptops and other mobile devices.

Incident Response & Forensics

- Security Incident Response On-site analysis of security incidents and attacks.
- Data Forensics Seizure, analysis and reporting of suspicious data or systems. Expert witness services as needed.