

Gigit's Compliance Services portfolio provides a suite of diverse services to assist the client's business in successfully completing and implementing industry compliance audits.

---

## Service Summary

Compliance security services are customized based upon the client's industry, their IT delivery model, and the compliance requirements of their industry.

Services available:

- Compliance Assessments
- Policy and Practice evaluations
- Policy & Process documentation creation
- Policy implementation support
- Training
- Recurring assessments and testing
- Remediation Services
- Sustainment services

## Gigit Responsibilities

- Develop a detailed Statement of Work with the Client that at a minimum specifies:
  - Scope of the work
  - Work locations and systems
  - Delivery schedules
  - Service delivery price
  - Change management terms
  - Any client specific terms or conditions
- Deliver the Statement of Work specified services on time and within the agreed upon price.

## AVAILABILITY

Gigit Services are available in the United States. If Client requests service outside of the United States, they may Contact gigit for a review of gigit's other delivery location options.

## PRICING AND ORDERING

Gigit customizes service delivery pricing based upon the client's business needs and requirements. A Statement of Work provides the detailed pricing. The Client may purchase a single gigit service, bundle multiple services, or purchase a subscription agreement for a period of no less than 1 year. The subscription provides for recommended recurring service delivery throughout the life of the subscription.

## FOR MORE INFORMATION

[info@gigitsecurity.com](mailto:info@gigitsecurity.com)

- Assign a single point of contact for the project to manage gigit delivery resources, report project progress from start to finish, and act as the gigit representative for resolution of any client or questions.

### **Client Responsibilities**

- Sign a gigit Master Sales Agreement (MSA)
- Sign a gigit Security Services Statement of Work
- Provide written approval for access to project specific IT systems and personnel.
- Identify an individual with the Client team to act as a single point of contact to coordinate and work with the gigit service delivery team

### **Gigit Service Deliverables**

Gigit develops a comprehensive engagement program that maps the client's internal compliance management approach against their specific industry's standards.

Gigit uses the 4PS as the foundation to build this program. These 4 represent the areas that must be in place for a long-term, professionally managed IT security program.

Gigit works with the Client to ensure that content and deployment exists in all 4 of these areas.

- Policies
- Plans
- Procedures
- Practices
- Standards

### **Gigit Supported Compliance Standards**

Gigit Compliance Services focus on assessment, audit preparation, and remediation for audit compliance of industry specific security standards.

These standards may be government regulatory, legal standards (required to do business), or both. Client's

customers may require validation that the client's business meets these standards prior to purchase.

### **Payment Card Industry (PCI-DSS)**

This international standard applies to any company that processes customer credit card information. Credit card providers must have credit PCI certification.

### **Health Information Technology for Economic and Clinical Health HITECH**

U.S. Legal requirement (law) – not applicable outside the U.S. Applies to any organization dealing with patient data (hospitals, practitioners, insurance companies).

### **Health Information Technology for Economic and Clinical Health (HITECH)**

Amendment to HIPAA Extensive focus on IT technology in relation to patient data tied to the NIST SP 800-66 HIPAA framework.

### **Sarbanes Oxley SOX**

A United States Federal Law that requires public traded companies to comply. Intended to protect shareholders and the general public from accounting errors and fraudulent practices and to improve the accuracy of corporate disclosures.

### **U.S. Federal Government**

The Federal government has numerous standards that contractors may have to comply. They include:

- Federal Information Security Management Act (FISMA) Include Federal contractors
- The Federal Risk and Authorization Management Program (FEDRAMP), a framework for IT cloud services providers.
- National Institute for Standards and Technology (NIST) NIST SP 800-171, NIST SP 800-53 Rev.4, NIST SP 800-37 for Risk Management

## U.S Department of Defense

- Cybersecurity Maturity Model Certification (CMMC) Audits and Assessments
- DFARS Compliance
- National Institute for Standards and Technology - NIST SP 800-171

## Privacy Compliance Standards

### General Data Protection Regulation GDPR

Regulation in EU law on data protection (no longer directive) Only affects U.S. companies when dealing with EU corporations or EU citizens.

### California Consumer Privacy Act CCPA

State Law in California protects Californian resident's personal data.

## Gigit Supported Compliance Frameworks

### ISO / IEC 27000 and 27001

International Information Security Standard Recognized by many governments and countries worldwide Extends beyond IT Formal certification process Accredited Registrars worldwide perform the audit and issue certification 3rd. Parties usually do the GAP analysis and preparation work

### NIST Cybersecurity Framework v1.1

For critical infrastructure including water and electric utilities.

## Service Organization Control SOC

American Institute of CPAs (AICPA)'s framework applicable for accounting firms and managed financial services firms.

Need more information?

[CONTACT US](#)



www.gigitsecurity.com  
4770 Baseline Rd., Suite 200  
Boulder, CO 80303

Phone: +1-844-374-4448, +1-844-37GIGIT