



## **Security and Compliance Program Overview**

TAG Solutions  
12 Elmwood Road  
Albany, NY 12204

## Program Overview

The TAG Solutions Security and Compliance program provides clients with a defense-in-depth strategy that ensures security of critical information assets and compliance with all required mandates. The Security and Compliance program provides the solutions necessary to preserve the confidentiality, integrity and availability (CIA) of client information assets, and ensure the regulatory, commercial and organization compliance mandates in force at each. The program focuses on information assurance at three layers: physical, personal and organizational.

The Security and Compliance program is designed to be a recurring cycle, beginning with discovery, assessment, remediation and finally, compliance. This cycle repeats, as new assets, vulnerabilities, patches, applications, employees, risks and other environment factors continuously move through their respective lifecycles.

The program is based on the following security principles:

- Confidentiality, Integrity and Availability (CIA) – The CIA Triad is a widely accepted methodology and benchmark for securing information assets. Confidentiality is the practice of restricting information access to authorized users. Integrity is the practice of ensuring the accuracy or trustworthiness of information. Availability is practice of ensuring that information is available according to stated requirements.
- Defense in Depth - Securing information and systems against the full spectrum of threats requires the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information technology. This is due to the highly interactive nature of the various systems and networks, and the fact that any single system cannot be adequately secured unless all interconnecting systems are also secured. By using multiple, overlapping approaches, the failure or circumvention of any individual defenses will not leave the system unprotected. Through training and awareness, well-crafted policies and procedures, and redundancy of protection mechanisms, layered protections enables effective protection of information technology for the purpose of achieving mission objectives.
- Reduction of Attack Surfaces – By reducing or eliminating the users, access, services, applications, computers and other inherently vulnerable components in a system, the aggregate risk of the system is reduced.
- Principle of Least Privilege – This principle is a widely recognize design philosophy that recommends granting, to a user, computer or application, the minimum privileges necessary to complete a task.

The TAG Solutions Security and Compliance program is based on the following industry standards:

- NIST 800 – This standard provides a foundation upon which organizations can establish and review information technology security programs. The principles in SP 800 are designed to provide the public or private sector audience with an organization-level perspective when creating new systems, practices, or policies.  
(<http://csrc.nist.gov/publications/PubsSPs.html>)
- ISO 27002 – The ISO standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains best practices of control objectives and controls in various areas of information security management.  
([http://www.iso.org/iso/support/faqs/faqs\\_widely\\_used\\_standards/widely\\_used\\_standards\\_other/information\\_security.htm](http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm))
- CIS – The CIS Benchmarks are widely accepted by U.S. government agencies for FISMA compliance, and by auditors for compliance with the ISO standard as well as GLBA, SOx, HIPAA, FERPA and other the regulatory requirements for information security.  
(<http://www.cisecurity.org/benchmarks.html>)
- COBIT – COBIT provides good practices across a domain and process framework and presents activities in a manageable and logical structure. The process focus of COBIT is illustrated by a process model that subdivides IT into four domains and 34 processes in line with the responsibility areas of plan, build, run and monitor, providing an end-to-end view of IT.  
(<http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981>)

The TAG Solutions Security and Compliance program is:

- Comprehensive – Information security has become a complex, ever-changing challenge for organizations of any size. To thoroughly protect information assets and maintain compliance, companies must employ a defense-in-depth strategy that addresses security risks from all levels and threats. The TAG Solutions Security and Compliance program is a comprehensive solution that addresses threats from all potential sources, and positions clients for regulatory, commercial and organizational compliance.
- Integrated – In addition to securing clients' information assets, the TAG Solutions Security and Compliance program is tightly integrated with TAG Solutions' other programs – Virtualization and Optimization, Storage and Data Management and Unified Communications (see Figure 1). This

merging of practice areas ensures that best practices are applied across disciplines, and efficiencies are realized throughout the implementation.

- Standardized – The TAG Solutions Security and Compliance program is based on proven industry standards – the same technologies and techniques in use by the United States Military, Fortune 500, and other heavily regulated industries. This philosophy ensures that TAG Solutions clients receive the most widely-established, highly-tested practices available.
- Proactive – In many areas, Security and Compliance program services are delivered cyclically, on a regular basis. Services are delivered proactively, which means that potential security risks, deviations and gaps are identified and remediated as early as possible.
- Managed – Wherever possible, Security and Compliance program services and devices are managed by TAG Solutions, ensuring the highest level of availability, performance and security.

Figure 1

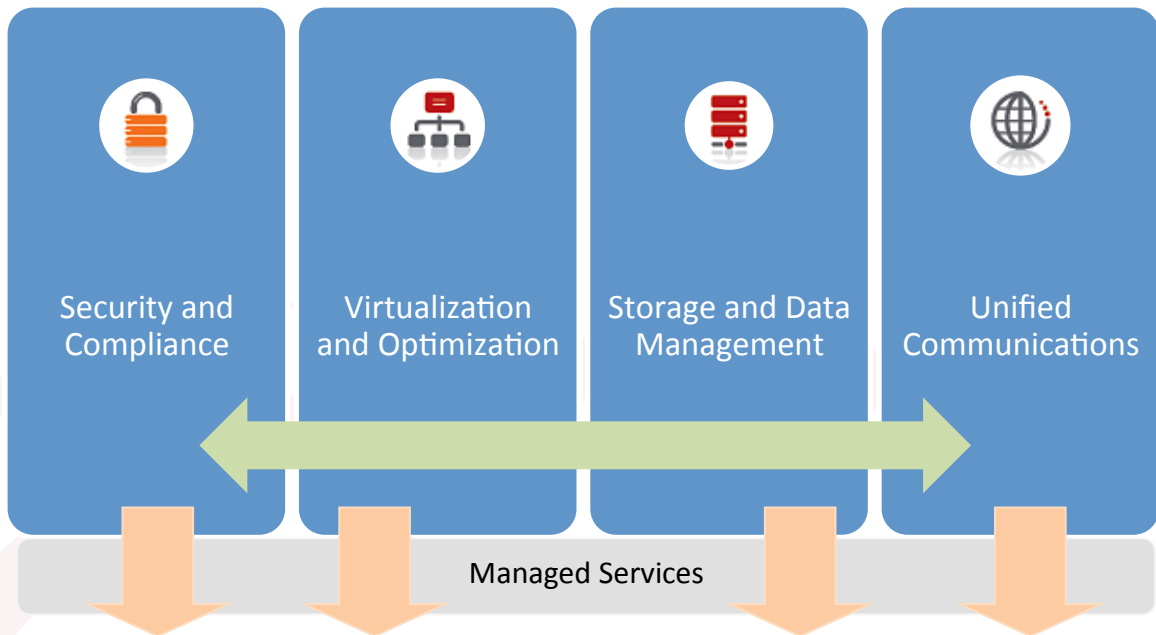
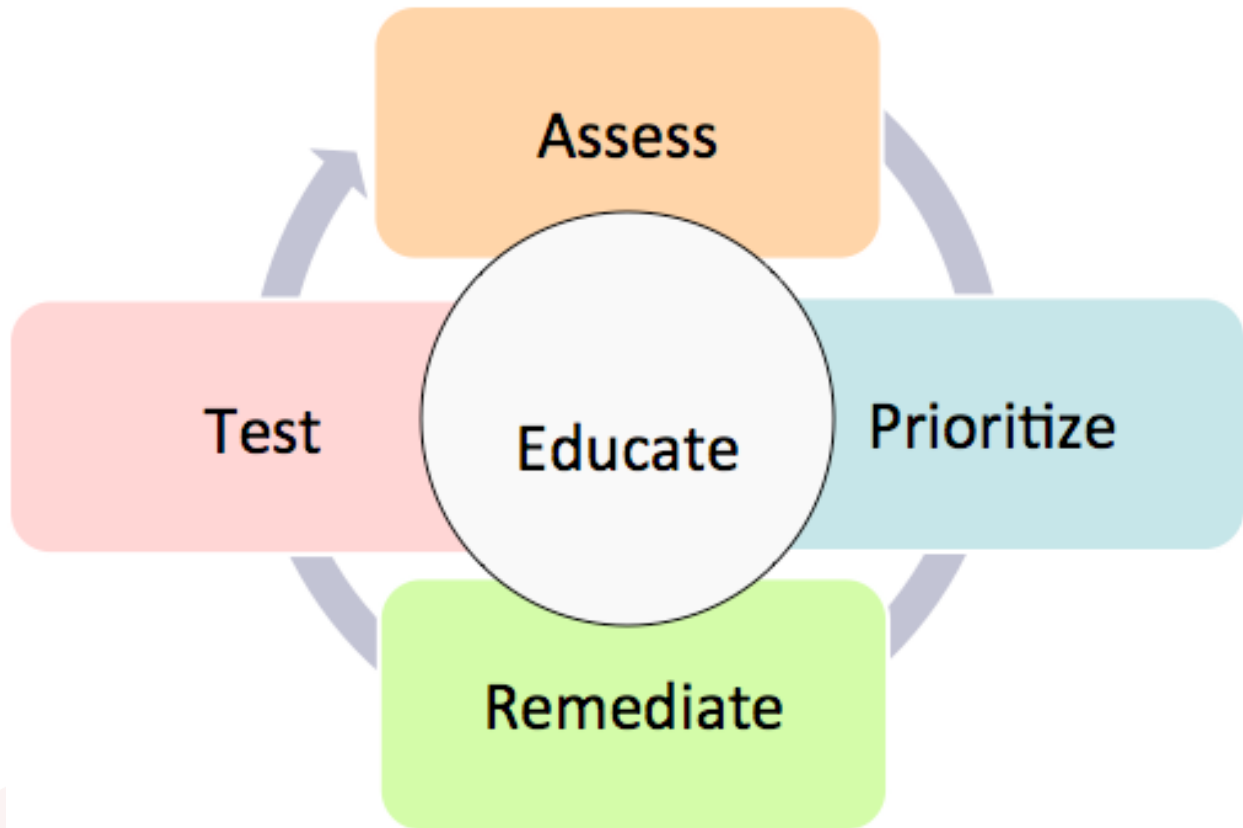


Figure 2 - Cycle of Trust



## Program Description

The Security and Compliance program provides the following solutions:

- Security
  - Awareness and Training
    - Organizational and personnel training regarding security concepts, principles and best practices
    - Presentations, onsite training, online training, posters, wallpaper, policies and procedures and other documentation development to assist with personnel development and awareness
  - Endpoint Security
    - Securing of endpoints (servers, desktops, routers, firewalls, virtual machines, mobile and other devices) through managed services, managed onsite appliances and on-premises hardware and software
    - Anti-virus, anti-malware and anti-spyware
    - Anti-spam
    - Whole disk encryption
    - Mobile security
  - Network Security
    - Securing of networks and transport mediums (internal, external) through managed services, managed onsite appliances and on-premises hardware and software
    - Virtual Private Networks (VPNs)
    - Web content filtering
    - Network Access Control (NAC)
    - Firewalling

- Intrusion Detection and Prevention (IDS/IPS)
- Wireless security
- Application Security
  - Securing of applications through implementation of best practices
  - E-mail and IM security
  - Web application security
  - Data Loss Prevention (DLP)
  - Multi-factor authentication
  - Identity and Access Management (IAM)
  - Backup and Recovery
  - High Availability Services
- Compliance
  - Assessment and Pre-Audit
    - Determination of risks, vulnerabilities and exposure through review and testing of cyber, physical and organizational structures
    - Assessment and pre-audit
    - Risk analysis
    - Vulnerability Management
    - Penetration testing
    - Social engineering and phishing
  - Regulatory, Commercial and Organizational Compliance

- Determination of regulatory, commercial and organizational compliancy level through review and testing of instituted processes and controls
- Assessment of existing policy and procedure efficacy through review of security controls and auditable artifacts
- Process and Controls
  - Policy and procedure development
  - Best practices implementation
  - Security Information and Event Management (SIEM)

## Certifications and Accreditations

TAG Solutions employs certified information security professionals who are dedicated to providing the highest quality security and compliance services.

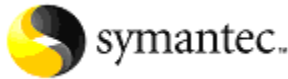
The TAG Solutions professional security and compliance team holds multiple certifications in the following:

- Certified Ethical Hacker (CEH)
- Global Information Assurance Certification: GSEC (GIAC:GSEC)
- Microsoft Certified Systems Engineers Security Specialty (MCSE+Security)
- Microsoft Certified IT Professional: Enterprise Administrator (MCITP:EA)
- VMware Certified Professional (VCP4)
- Cisco Certified Security Professional (CCSP)
- Certified SONICWall Security Administrator (CSSA)
- Symantec Technical Specialist (STS)
- CompTIA A+
- CompTIA Security+
- PGP Certified Technician

## Partners

In addition to leveraging industry best practices and employing the highest caliber professionals, TAG Solutions partners with best-of-breed hardware and software vendors to ensure that clients receive comprehensive, yet cost-effective security and compliance solutions.

The following is a sampling of TAG Solutions' security and compliance partners:



**Symantec**  
[www.symantec.com](http://www.symantec.com)

Symantec helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance.



**MessageLabs**  
[www.messagelabs.com](http://www.messagelabs.com)

MessageLabs, now part of Symantec, provides a range of managed services to protect, control, encrypt and archive electronic communications. Listed as a leader in the Gartner Magic Quadrant and many other analyst reports, and with more than 21,000 clients ranging from small business to the Fortune 500 located in more than 100 countries, MessageLabs services are widely recognized as a market leader in the messaging and web security market.



**Cisco**  
[www.cisco.com](http://www.cisco.com)

The Self-Defending Network is Cisco's long-term strategy to protect an organization's business processes by identifying, preventing, and adapting to threats from both internal and external sources. This protection helps organizations take better advantage of the intelligence in their network resources, thus improving business processes and cutting costs.



**SonicWall**  
[www.sonicwall.com](http://www.sonicwall.com)

Founded in 1991, SonicWALL, Inc. designs, develops, and manufactures network security, secure remote access, Web and e-mail security, continuous data protection, and policy

and management solutions. Offering appliance-based products as well as value-added subscription services, our comprehensive array of solutions provide enterprise-class Internet and data protection without any compromises.



**PGP**  
[www.pgp.com](http://www.pgp.com)

PGP Corporation is a global leader in email and data encryption software for Enterprise Data Protection. Based on a unified key management and policy infrastructure, the PGP® Encryption Platform offers the broadest set of integrated applications for enterprise data security.



**RSA**  
[www.rsa.com](http://www.rsa.com)

RSA, the Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.