



WHITE PAPER

VeriSign® Global Security Consulting

Optimizing Enterprise Information Security Compliance



**CONTENTS**

+ The Rise in Compliance Audits	3
+ Addressing Compliance Challenges	4
+ Using Consultants Strategically	5
+ Choosing a Consultant	6
Regulatory Expertise	6
Vendor Neutrality	6
Experience of the Delivery Team	6
Financial Stability	7
+ VeriSign's Strategic Consulting Services for Optimizing Compliance	7
Programs and Processes	7
Policies, Standards, and Procedures	7
Contract Subject Matter Expertise	7
Managed Security Services	8
+ The VeriSign Difference: Expertise, Intelligence, Trust	8
Seasoned Practitioners	8
Customer Focus	8
World-Class Support for Best-of-Breed Solutions	9
Global Scale and Intelligent Infrastructure	9
Stability and Trust	9
+ Overview of VeriSign Global Security Consulting	9
+ Conclusion	10
+ Learn More	10



VeriSign® Global Security Consulting

Optimizing Enterprise Information Security Compliance

Businesses are required to perform an increasing number of annual audits and assessments. The information security requirements of these multiple audits are growing as well, both in number and complexity. Such pressures force companies to incur costs, in terms of investments in the necessary technology, processes, and resources needed to comply with and support multiple audits. VeriSign® Global Security Consulting helps companies streamline their compliance and auditing efforts by reducing duplication of effort across multiple audits and by ensuring that companies properly prepare and organize documentation for quick and efficient compliance auditing. The consulting team leverages industry-leading experience and expertise, and acts as a trusted advisor to build programs and processes geared specifically toward facilitating compliance with regulatory and partner requirements and to provide objective advice on security processes and technology. Using Global Security Consulting to optimize information security compliance and auditing, companies can minimize risk, focus on core business goals, and confidently pursue new business opportunities.

+ The Rise in Compliance Audits

The number of information security regulations has risen significantly in recent years. Companies must now contend not only with internal, federal, and industry-specific regulations and policies, but also with the security practices and requirements of their networked partners, suppliers, and customers. Compliance does not end with implementing appropriate security measures; it also entails providing auditable records that verify compliance. As government, industry, and networked business partners increasingly specify security requirements, companies can face a commensurate increase in third-party security assessments.

A typical company may be required to provide proof of compliance to a number of different organizations and agencies. Tracking, managing, and producing such reports, especially for multiple entities, is difficult enough. Adding to the complexity, each regulating entity has its own unique standards for compliance and auditing, often forcing companies to implement and manage multiple, disparate compliance and reporting mechanisms. When a company fails to comply with a particular standard, the relevant entity often submits non-compliant areas for corrective action, leading to further organizational impact. Meeting compliance requirements, servicing audits, and responding to unfavorable results has become a significant source of expense and disruption for most organizations today.

Requirements, Requirements, and More Requirements

Depending on its industry sector and public corporation status, a company may be regulated by some or all of the following entities, acts, and standards: the Federal Financial Institutions Examination Council (FFIEC); the Office of the Comptroller of the Currency (OCC); the Sarbanes-Oxley Act; the Payment Card Industry (PCI) Data Security Standard (DSS), which evolved from VISA CISP and MasterCard SDP regulations; Federal Energy Regulatory Commission/North American Electric Reliability Council (FERC/NERC) Cyber Security Urgent Action Standard (UAS) 1200; and others. The company may also have to contend with consumer privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and security breach reporting laws such as the California Security Breach Notice Act (formerly SB 1386).

In addition, business partners that provide either online application access or Web service application programming interfaces (APIs) may require each other to not only demonstrate alignment with standards of “good practice” (such as those specified by the ISO 17799, the Information Security Forum’s Standard of Good Practice, Control Objectives for Information and related Technology [COBIT®], the Treadway Commission, the IT Infrastructure Library [ITIL], and the National Institute of Standards and Technology [NIST]), but also to perform periodic Statement on Auditing Standards (SAS) -70 assessments. If the company provides credit information or does business with financial institutions and insurance companies, it may also be required to provide such entities with detailed information on security and privacy controls over information resources.

The alternative—non-compliance—is not attractive. Although some regulatory requirements are difficult to quantify and enforce, others have clear-cut stipulations and penalties. Depending on the requirement, failure to comply or to provide auditable records can have serious financial and legal consequences. These consequences are in addition to the liabilities caused by compromised data, damaged reputations, and loss of trust, should a company become compromised by a breach in security. For example, non-compliance with the Sarbanes-Oxley Act can result in fines and imprisonment for up to 20 years; non-compliance with the VISA CISP, MasterCard SDP, and PCI programs can result in a \$50,000 fine for a first violation; and non-compliance with the Health Insurance Portability and Accountability Act (HIPAA) calls for a \$100,000 fine and up to 10 years in jail.

+ Addressing Compliance Challenges

To achieve compliance with multiple regulations in this complex environment, and then to be able to verify compliance to the relevant parties, companies must take the following measures:

- **Implement carefully devised technology and process controls** (e.g., personnel controls, physical and logical access controls, and legal and contractual controls). These controls should be efficient, clear-cut, and easily duplicated, and they must be immediately transferred when a new user, technology, or information is added. As much as possible, these controls should be automated.
- **Document and organize compliance efforts to demonstrate compliance details to auditors.** This includes implementing consistent, repeatable systems for quantifying, tracking, analyzing, demonstrating, and reporting on compliance.
- **Enable auditors and assessors to validate documentation (audit servicing).** This includes maintaining an audit data repository and enabling validation. First and foremost, companies must be able to collect and compile assessment data in a format that can be extracted easily and shared efficiently and confidentially. Validation may involve spot-auditing application usage, reviewing information retention practices, examining user-authorization records, and inspecting technical configurations.

Ideally, the preceding measures should be delivered via a flexible, low-impact solution that maps to the unique technical and business requirements of each internal organization, while providing the flexibility needed to address future regulation and growth. Realistically, though, few companies have adequate internal resources to create a solution structure that addresses every aspect of compliance and documentation—especially when they face multiple regulations and disparate technologies, and when they are driven by diverse business needs.

For this reason, companies usually leverage some combination of the following resources:

- **Full-time information security staff** – In-house security personnel are generally responsible for day-to-day information security. They have the most comprehensive, intimate knowledge of the organization’s security technology, configurations, and policies.
- **Functional business units with security responsibilities** – Other IT-focused internal organizations (e.g., network engineering, application development, and network operations) are not primarily tasked with information security but often play a supporting role in compliance efforts.

In recent years, members of the U.S. Congress sought to establish a minimum standard for corporate security controls through the introduction of the Putnam Bill (also known as the Corporate Information Security Accountability Act of 2003). Instead of enacting this expensive, disruptive standard and enforcing it through audit and attestation, lawmakers tabled the bill in favor of allowing U.S. corporations to “self-regulate” for the time being. Ultimately, in order to simplify compliance and auditing, the private sector, government agencies, and standards bodies will have to work together to develop a common standard for information security.

- **Managed security services providers** – These third-party providers usually handle ongoing, specific aspects of compliance, for example, network monitoring and intrusion detection.
- **Consulting or contract resources** – Information security consultants are normally engaged on a short-term basis to perform assessments, validate architecture designs, define processes, render advice on technology solutions, and provide remediation services for non-compliance problems.

+ Using Consultants Strategically

Organizations choose different resources for different aspects of compliance, for a variety of reasons. Personnel and time constraints, cost, and the magnitude of the compliance effort all factor into the delivery of compliance solutions. In the arena of compliance and auditing, however, outside consultants render unique advantages that in-house solutions cannot provide. By using consulting services strategically, companies can optimize the effectiveness, efficiency, and scalability of their compliance solutions.

Qualified information-security consultants provide the following advantages:

- **Third-party objectivity** – To comply with internal, partner, and industry-specific regulations, companies may need the third-party non-repudiation and auditing capabilities that only an external, unbiased service can provide.
- **Staffing and skill set** – While existing security staff may lack the time, experience, or insight to tackle additional security projects, security consultants can be more objective and more focused. They encounter a broad range of security issues and environments in their daily work, giving them experience that would be difficult to accumulate working within a single company. In addition, they are up-to-date on—and conversant in—the myriad of government and industry compliance and auditing requirements.
- **Trust** – The involvement of a security consultant with a proven track record and global name recognition can help establish trust between a business and external users who may not be well-acquainted with (or confident of) the company and its compliance and auditing capabilities.
- **Intelligence** – Security consultants and managed service providers tend to have faster, more comprehensive access to information about network vulnerabilities, impending attacks, and solutions. This information allows them to quickly address or respond to problems that could affect security and compliance.
- **Cost and time savings** – It is often less expensive to outsource key tasks to a third party than to invest in in-house experts, technology, and 24/7 operation centers. Because security is their core business, compliance and auditing consultants can justify heavy investment in highly qualified staff, ongoing training, and state-of-the-art assessment and monitoring technology. In addition, technology, methodology, and personnel are already proven and in place, saving valuable time when first deploying a compliance or auditing solution or responding to a request for corrective action.

+ Choosing a Consultant

When researching and planning a compliance solution, companies must objectively weigh their own capabilities against the advantages of engaging information security consultants. If their evaluation indicates the need for security consultants, the next step is choosing the right consultant for the job.

When selecting a security partner to deliver compliance and auditing solutions, companies should carefully consider the following criteria:

- Regulatory expertise
- Vendor neutrality
- Experience of delivery team
- Financial stability

Regulatory Expertise

Compliance and auditing consultants should have a firm grasp of every regulation, policy, or standard for which compliance is sought. They should thoroughly understand not only the intricacies of the regulation itself, but also the related methodologies, processes, and technologies available to implement, test, and demonstrate compliance. They should be able to recognize and apply compensating controls that meet the spirit, if not the letter, of the regulation or standard. And, they should have sufficient experience to anticipate—and create solutions that accommodate—the imposition of additional, related regulations.

Vendor Neutrality

To contain costs, ensure proper execution, and build best-of-breed solutions, the consultant's processes and technology should work easily with the company's existing infrastructure and third-party products. This includes not only easy integration of tools and technology with existing software and hardware. It also extends to working with the existing corporate culture and understanding the security limitations and requirements of the company's core business. To ensure this will happen, companies should choose consultants who take a vendor-neutral approach to the technologies they recommend.

Experience of the Delivery Team

Given the significant risk associated with improper handling of compliance issues, it is imperative that the team delivering compliance and auditing solutions has wide-ranging, deep expertise in not only information security, but also security-related regulations and standards. In addition, consultants should have real-world experience tailoring compliance solutions for geographically dispersed, functionally diverse organizations within the company; unifying disparate policies and processes across the enterprise; and developing repeatable methodologies for tracking, analyzing, and reporting compliance data. Compliance consultants should be Certified Information Systems Security Professionals (CISSPs) and/or Certified Information Systems Auditors (CISAs). They should receive continuing education, have an in-depth understanding of the concepts of IT defense, and be able to apply their skills appropriately for each specific task. Finally, consultants should be able to leverage a built-in mechanism for receiving alerts, reports, and analyses of regulatory changes.

Financial Stability

A financially sound service provider has the resources to invest in, develop, and maintain leading-edge services. It attracts the most highly qualified personnel and provides ongoing training to ensure up-to-the-minute skills. Finally, it can position itself for longevity, ensuring that services and support will continue to be available over time. To gauge viability, consider financial records, partnerships and alliances, awards and achievements, brand recognition, and length of time in business.

+ VeriSign Global Security Consulting: Strategic Solutions for Optimizing Compliance

As a trusted provider of information-security services, VeriSign Global Security Consulting leverages its regulatory knowledge, vendor neutrality, subject matter expertise, and financial stability to deliver strategic consulting services that optimize compliance and auditing solutions. VeriSign consultants help optimize the structure of a company's compliance and auditing efforts by analyzing each requirement and then objectively matching it to potential solutions. VeriSign security professionals develop and implement sound, practical programs that take into account the business requirements, limitations, and culture of real-world businesses.

The comprehensive, customized compliance solutions offered by VeriSign strategically combine the following components:

- Programs and processes
- Policies, standards, and procedures
- Contracted subject matter expertise
- Managed security services

Programs and Processes

VeriSign Global Security Consulting determines the critical programmatic elements and processes required in a corporate environment, and develops solutions appropriate to cost, culture, and technology. Examples are information-security governance, staffing models, budgeting, development oversight and accreditation processes, monitoring strategies, and incident-response processes.

Policies, Standards, and Procedures

VeriSign consultants build policies that are aligned with regulatory requirements and guide corporate information protection activities. Technology security standards are integrated with policy and provide a higher level of detail on achieving compliance. Baseline security procedural guides are detailed instruction manuals that specify approved configuration settings for the technology deployment process.

Contracted Subject Matter Expertise

VeriSign consultants can be staffed into temporary or semi-permanent roles to provide critical subject matter expertise and skills that may be difficult for companies to attract and retain in house. Contract engagements include design review, security awareness training on special topics, incident response and forensic investigation, security testing and evaluation, and more.

Case Study—Strategic VeriSign Engagement Enables Rapid Remediation

The following case study summarizes how the VeriSign Global Security Consulting team helped a financial transaction services company quickly remediate audit findings related to security monitoring and response—while minimizing personnel costs associated with the solution.

Client: Transaction processing software and service provider; \$1 billion revenue; 3,000 global employees

Challenge: The VeriSign client needed to make immediate progress in compliance with audit findings from the Federal Financial Institutions Examination Council (FFIEC), a major credit card company, and partner institutions. One key audit issue was the lack of security monitoring and response capabilities. The client determined that, given internal resource constraints, the most cost-effective, efficient, and immediate remedy was to engage VeriSign Global Security Consulting to quickly evaluate, select, and deploy a solution. A key success criterion was the minimization of human resource costs for any solution deployed.

Approach: VeriSign consultants performed a functional and security requirements analysis. Using this analysis, the team prepared the following components:

- A monitoring architecture, which addressed critical applications and perimeters, and utilized existing network design to minimize the cost of supporting switches and taps
- A test plan to objectively evaluate products against the requirements
- A decision matrix, based on the degree to which host/network intrusion detection system (IDS) and security information management (SIM) products met requirements

Managed Security Services

VeriSign® Managed Security Services provide levels of security management and monitoring that may be too expensive or too resource-intensive to perform internally. VeriSign manages and monitors firewalls, host- and network-based intrusion detection sensors, and operating system logs. Data is correlated and presented through the highly-available VeriSign® Enterprise Security Portal, and service level agreements determine the escalation event sequence.

The end result of a VeriSign compliance engagement is an information-security program that provides all the required components, along with appropriate documentation and validation materials, organized for efficient review during audits and assessments.

+ The VeriSign Difference: Expertise, Intelligence, Trust

Although many vendors offer consulting services to companies seeking compliance and auditing solutions, few providers can match the expertise, intelligence-gathering capabilities, and commitment to open standards that VeriSign brings to the table, and few providers are capable of taking on the role of a vendor-neutral trusted advisor. VeriSign Global Security Consulting leverages exceptional regulatory knowledge, training, and experience; best-of-breed solutions; and a global network of proven technology. VeriSign has a history of stability and trust, and can deliver compliance and auditing solutions that are not only effective, but also make efficient use of existing in-house personnel, technology, and processes.

Seasoned Practitioners

VeriSign security professionals are trained, certified, and experienced in the design, acquisition, and deployment of all major security solutions. With an average of ten years' experience in enterprise information security, and having conducted many security and audit certifications, VeriSign consultants demonstrate expertise across the entire information security and privacy spectrum. Ongoing training and periodic re-certification ensure that consultants maintain a world-class skill set and knowledge base. Membership and participation in standards bodies such as the Information Security Forum and Internet Security Alliance provides additional expertise in regulatory compliance.

The VeriSign consulting team combines skill and training with proven, real-world experience. More than half of VeriSign Global Security Consulting engagements center on security assessments, and most consulting service customers are in regulated industries (mainly financial services, healthcare, and retail). The consulting team has performed numerous HIPAA, GLBA, and other regulatory assessments and is also a leading provider of PCI assessments.

Customer Focus

The consulting team works with enterprises of all sizes, all over the world, from government agencies and Fortune 1000 companies to small start-ups and family-owned businesses. VeriSign customers include municipal, state, and federal agencies; financial institutions; healthcare organizations; telecommunications carriers; and online retailers. The security team's expertise, dedication, and focus on customer service help ensure that each customer not only gets a real-world solution that meets its unique requirements, but also receives prompt attention when security events, remediation requests, or other issues arise.

The VeriSign Global Security Consulting team prepared, administered, and tallied results of a Request for Proposals (RFP), which was submitted to five IDS vendors and three SIM vendors. Based on RFP responses, two IDS vendors and one SIM vendor were selected for requirements testing. An open-source network IDS was also tested. Host IDS agents for all vendors were installed on all platforms targeted for monitoring, and network IDS sensors for all vendors were configured, along with management consoles. The selected SIM system was installed and configured to accept input from IDSs, system logs, and firewalls. VeriSign consultants then performed a suite of tests designed to rate each product's performance against criteria specifically developed for the client, and the ability of the SIM to remove false positives, de-duplicate, and correlate the information into meaningful alerts.

After the testing and subsequent product selection, VeriSign consultants performed procurement and legal oversight to purchase the hardware and software. VeriSign managed the deployment project in cooperation with internal resources and vendor professional services. VeriSign consultants also designed an incident response plan and trained participants in its execution. Finally, VeriSign consultants prepared an auditor's guide, which documented the processes for product evaluation and selection and described the monitoring architecture itself, including details on monitored resources and device configuration.

World-Class Support for Best-of-Breed Solutions

VeriSign delivers world-class services to enterprise customers by leveraging industry-leading technology; skilled experts; structured processes; and unique intelligence. As a services company, VeriSign focuses solely on designing and deploying compliance and auditing solutions that meet the specific requirements of its customers and maximize the effectiveness of their existing security investments.

Global Scale and Intelligent Infrastructure

As the leading provider of intelligent infrastructure services, VeriSign has unique visibility into global security patterns, trends, and threats on the Internet. VeriSign Global Security Consulting professionals can extract and assimilate information not only from VeriSign Managed Security Services, but also from data gathered from its global Domain Name System (DNS), secure sockets layer (SSL), and enterprise public key infrastructure (PKI) services. Leveraging this data and automated processes, VeriSign consultants conduct highly informed assessments and can be "first off the mark" in providing companies with visibility into worldwide Internet-related events. This capability is crucial for identifying threats before they become attacks, and preventing and responding to events that threaten compliance.

Stability and Trust

VeriSign is the leading provider of intelligent infrastructure services in support of the Internet, telecommunications, and next-generation networks. It has maintained critical intelligent infrastructure such as the Domain Name System (DNS) with 100 percent availability for more than ten years. VeriSign is often referred to as one of the Internet's "nerve centers," and two VeriSign security operations centers (SOCs) have been designated Critical Infrastructure Assets by the Department of Homeland Security.

+ Overview of VeriSign Global Security Consulting

Compliance and auditing optimization is only one facet of VeriSign Global Security Consulting. VeriSign blends unmatched expertise with world-class program management and state-of-the-art technology to provide a comprehensive suite of network consulting services. VeriSign enhances network operations through proven, business-focused solutions that help companies utilize their network and data resources to more fully realize their immediate and long-term business goals.

VeriSign Global Security Consulting includes the following services:

- **VeriSign® Technical Security and Risk Assessments** – Assessment services range from enterprise-wide evaluations to individual program and code reviews. They include detailed security assessments, network and application vulnerability assessments, and penetration tests.
- **VeriSign® Enterprise Risk and Compliance Assessments** – These assessments assist companies in meeting their compliance objectives by identifying the overlap between best practice standards and industry-specific requirements. VeriSign recommends practical measures to align security practices with specific compliance and business objectives, including compliance with federal regulations related to data sharing.
- **VeriSign® Security Policy and Program Services** – These services help companies develop, improve, or communicate security policy and strategy. VeriSign Global Security Consulting professionals assist companies with the entire lifecycle of enterprise security programs and policies.

Results: At the conclusion of the effort (which had a total duration of less than six months), the client achieved compliance with the FFIEC requirements involving monitoring and incident response. In addition, the solution met the client's requirement to minimize resources for monitoring operations: Operation of the monitoring infrastructure requires only one administrator, and alerts are routed to network operations center (NOC) personnel via an automated ticketing system for first response.

- **VeriSign® Architecture and Design Services** – From complex network implementations to firewall and application integration, the VeriSign Global Security Consulting team designs and implements a security solution for technology, industry requirement, or business models.
- **VeriSign® Incident Response and Forensics Services** – VeriSign employs a detailed and comprehensive methodology for responding to computer security incidents.
- **VeriSign® Business Continuity and Disaster Recovery Services** – Leveraging its extensive experience in providing critical Internet infrastructure services, VeriSign helps companies design programs to maintain the 24/7 uptime and effectiveness of their network infrastructure; it also provides solutions for addressing disaster recovery issues.
- **VeriSign® Identity and Access Management Services** – VeriSign helps companies assess, design, and deploy cost-effective and scalable identity management, authentication, and access-control solutions that leverage existing security investments.

+ Conclusion

Information-security compliance and auditing is becoming an increasingly complex task. Companies must contend with not only government and industry-specific regulations, but also the security policies and practices of business partners, suppliers, and customers. Few organizations have the internal resources to create a comprehensive compliance and documentation solution in house. For this reason, they should consider strategically engaging information security consultants, who often offer inherent advantages over in-house solutions. These advantages include objectivity, expertise, and time and cost savings.

VeriSign Global Security Consulting leverages exceptional regulatory knowledge, seasoned practitioners, best-of-breed solutions, global data-gathering capabilities, and role as trusted advisor to help companies optimize their compliance, auditing, and remediation solutions. Using VeriSign consultants strategically, companies can implement effective, efficient compliance and auditing mechanisms that allow them to return focus to their core business.

VeriSign is positioned in the Leaders Quadrant of the August 2007 “Magic Quadrant for MSSPs, North America, 1H07” Gartner report.

+ Learn More

For more information about VeriSign Global Security Consulting, please call 650-426-5310, email enterprise_security@verisign.com, or visit us at www.Verisign.com.

Visit us at www.Verisign.com for more information.

©2007 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, the checkmark circle, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. COBIT is the registered trademark of the IT Governance Institute. All other trademarks are the properties of their respective owners. The Magic Quadrant is copyrighted August 2007 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the “Leaders” quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

00017418 06-05-2006