



**SOLUTION
OVERVIEW**



VeriSign® Security Services Compliance Solutions



Where it all comes together.™



CONTENTS

+ VeriSign® Security Services Compliance Solutions	3
Addressing Compliance Strategically	3
+ Compliance Dynamics	
+ VeriSign® Compliance Solutions: Applied Intelligence, Cost-Effective Control	4
VeriSign Services-to-Requirements Map	4
VeriSign® Global Security Consulting	4
VeriSign® Managed Security Services	8
VeriSign® Unified Authentication	11
VeriSign® Messaging Security and Compliance Services	12
+ The VeriSign Difference	13
+ For More Information	13
+ About VeriSign	13



VeriSign® Global Security Consulting Services

KEY BENEFITS

Expertise

VeriSign security experts have been helping companies with their compliance requirements for more than a decade.

Service-oriented solutions

Just having a product installed is insufficient for compliance. It must be monitored and managed, and incidents must be responded to. VeriSign is not a product company. It focuses entirely on providing services, which many core compliance elements require.

Lower total cost of ownership

VeriSign's service-based model can help reduce the need for capital investment and outsources maintenance and upgrades.

Intelligence

VeriSign's unique visibility into emerging security patterns, trends, and threats, allows companies to proactively prevent and respond to events that threaten compliance.

Vendor neutrality

Open standards-based technology allows companies to leverage existing systems and resources.

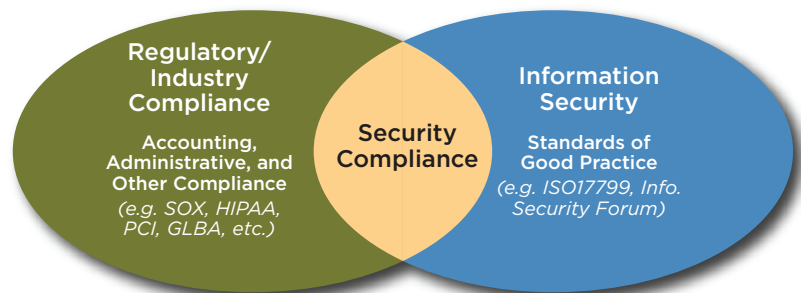
Trust

Organizations gain the value of VeriSign's trusted name and its reputation for strong security, high availability, and sound policies—attributes that provide a solid starting point for working with compliance officers and regulators.

Addressing Compliance Strategically

Corporate officers responsible for security and risk management face a challenging and complex environment. Regulatory compliance is not new by any means, but the past several years have seen increased spending on compliance as a component of overall risk management. As compliance requirements increase in scope and complexity, security professionals must implement flexible solutions that accommodate an ever-changing security landscape without unduly taxing existing infrastructure, personnel, and other resources.

VeriSign® Security Services offers a comprehensive suite of Compliance Solutions allows you to address compliance from the standpoint of an overall strategy instead of using products that grapple with compliance one requirement at a time. Our core offering of compliance-oriented services maps to multiple standards and regulations, while providing the scalability and flexibility to adapt to future requirements. By leveraging VeriSign's expertise, global intelligence, and proven technology, you gain a compliance solution that not only is cost-effective and quick to deploy, but also stands on VeriSign's reputation for trust—a valuable differentiator for customers, business partners, and regulators.



+ Compliance Dynamics

Achieving and maintaining compliance with a particular law, regulation, or standard requires a fluid strategy that revolves around two overlapping spheres of control:

- Compliance foundation – The building blocks (i.e. programs, policies, procedures, and access controls) of compliance
- Compliance management and monitoring activities – The ongoing tracking and monitoring activities that help ensure that changes in the internal and external environment are reflected and addressed in the company's compliance program

Most building blocks for any compliance strategy are classic security components such as policies, security awareness, access control, and encryption. Many of these components are laid out in the International Organization for Standardization (ISO) Code of Practice for Information Security Management 17799 (ISO 17799), which has been an industry accepted framework for many years. For the most part, organizations with good security programs based on ISO 17799 already have the right building blocks for compliance.



Ongoing compliance activities present the larger challenge. Monitoring events for potential risks and threats can entail examining voluminous data from logs, network devices, servers, and applications. In addition, most key regulations and standards require organizations to have the means not only to identify vulnerabilities, threats, and attacks, but also to respond appropriately. New vulnerabilities are discovered daily—in operating systems, and also in applications that reside on an otherwise-secure host. Organizations must perform regular testing to identify these vulnerabilities and threats.

+ VeriSign® Compliance Solutions: Applied Intelligence, Cost-Effective Control

VeriSign® Compliance Solutions help you assess, optimize, implement, and manage the building blocks and ongoing activities required for compliance. A natural extension of VeriSign's core competencies, the solutions suite includes consulting, managed security, authentication, and email security services that map to today's key regulatory and industry requirements. Using VeriSign's world-class security consultants and industry-leading managed services, you not only alleviate the cost and complexity of compliance, but also gain a strategic, multi-pronged solution that can be applied time and again to meet new or evolving requirements.

The following sections outline the VeriSign suite of Compliance Solutions. The presentation begins with a mapping of key regulations and standards to VeriSign's service offerings. It is followed by descriptions of VeriSign's leading compliance-oriented offerings.

VeriSign Services-to-Requirements Map

Evaluating the efficacy of your compliance foundation and ongoing compliance activities requires an understanding of details within the regulations and supporting standards. It is important to note that the “whats and hows” of information security compliance are often not found in the regulations themselves. For that matter, supporting standards and interpretations must often be consulted.

The matrices on the following pages shows the ways VeriSign services can help address key regulatory and industry requirements.

VeriSign® Global Security Consulting

As a trusted provider of information security services, VeriSign® Global Security Consulting leverages regulatory knowledge, vendor neutrality, subject matter expertise, and state-of-the-art technology to deliver strategic consulting services that optimize compliance and auditing solutions. The VeriSign Global Security Consulting team offers assessment and certification services, as well as customized compliance solutions that match applicable requirement to the best possible solution for your company.

VeriSign® Security Certification Program

Consumers and business partners are increasingly considering security when deciding with whom to do business. Communicating security and compliance can help differentiate your offerings to obtain preferred partner status, build brand equity, and increase sales.

Bottom Line: The VeriSign® Security Certification Program is the flagship VeriSign compliance offering. It allows companies to communicate their compliance status to customers, business partners, and other third parties.

COMPLIANCE SOLUTIONS: REGULATIONS	SARBANES-OXLEY SEC. 404 / ITGI STANDARDS ¹	GRAMM-LEACH-BLILEY ACT (GLBA)	HEALTH INFORMATION PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)	CALIFORNIA NOTICE OF BREACH / FORMERLY SENATE BILL 1386 (SB1386) AND SIMILAR DISCLOSURE / NOTIFICATION LAWS
CONSULTING ASSESSMENTS	<p>ITGI Key Controls: Requires a variety of assessments to be performed on a regular basis.</p> <p>Applies to: Application testing, infrastructure assessment, and configuration assessment.</p>	<p>GLBA Key Controls: Requires a regular risk assessment. Requires major changes to infrastructure undergo technical and non-technical evaluations. Requires documented policy and procedures.</p> <p>FFIEC² Key Guidelines: Several risk assessments to determine the appropriate controls for given situations.</p> <p>Applies to: Non-public personal information (NPI) applications, servers, databases, and network devices.</p>	<p>HIPAA Key Control: Requires a regular risk assessment (assumed to be annually). Requires that major changes to infrastructure undergo technical and non-technical evaluations.</p> <p>Applies to: All systems storing, transmitting or processing regulated data—electronic protected health information (ePHI.)</p>	<p>SB1386 Key Controls: A focused assessment on encryption, intrusion detection, response, and notification capabilities may be appropriate to assess compliance CA Notice of Breach.</p> <p>Applies to: All systems storing, transmitting or processing regulated data—personally identifiable information (PII.)</p>
HOST LOG FILE MONITORING	<p>ITGI Key Controls: Requires logs be captured, monitored, and responded to and be retained at least one year.</p> <p>Applies to: Financial systems (and supporting controls.)</p>	<p>GLBA Key Controls: All access (access to the record by a person or user - view, read, write, delete) to personal information needs to be logged.</p> <p>Applies to: NPI applications, servers, databases, and network devices.</p>	<p>HIPAA Key Controls: All access (access to the record by a person or user - view, read, write, delete) to personal information needs to be logged.</p> <p>Applies to: ePHI applications, servers, databases, and network devices.</p>	<p>SB1386 Key Controls: No specific requirements for host log file monitoring, but the lack of this control may make the entity at risk of "Substitute Notification" which can be challenging to a company in terms of cost and reputation.</p> <p>Applies to: PII applications, servers, databases, and network devices.</p>
MANAGED VULNERABILITY PROTECTION SERVICE (MVPS)	<p>ITGI Key Controls: Requires regular assessment of network and application level vulnerabilities.</p> <p>Applies to: Financial systems (and supporting controls.)</p>	<p>GLBA Key Controls: No specific requirements for regular vulnerability scanning but requires regular technical and non-technical evaluation which MVPS can help satisfy.</p> <p>Applies to: All systems storing, transmitting or processing NPI.</p>	<p>HIPAA Key Controls: No specific requirements for regular vulnerability scanning but requires regular technical and non-technical evaluation which MVPS can help satisfy.</p> <p>Applies to: All systems storing, transmitting or processing ePHI.</p>	<p>SB1386 Key Controls: No specific requirements for regular vulnerability scanning.</p>
INTRUSION DETECTION SERVICE	<p>ITGI Key Controls: Requires intrusion detection system (IDS) as a core requirement for network security. Events should be stored for at least one year.</p> <p>Applies to: Host and network-based IDS or intrusion prevention system (IPS.)</p>	<p>FFIEC Key Guidelines: Require both the capability to detect potential intrusions and the placement of intrusion detection devices.</p> <p>Applies to: All systems storing, transmitting or processing regulated data (non-public personal information.)</p>	<p>HIPAA Key Control: No distinct requirement for network intrusion detection systems (NIDS) though requires monitoring and intrusion detection as part of a means to identify and respond to security incidents. Requires host-based intrusion detection systems (HIDS) to provide system integrity.</p> <p>Applies to: All network segments and systems storing, transmitting or processing ePHI.</p>	<p>SB1386 Key Controls: Does not have a distinct requirement for IDS, although methods of intrusion detection as part of a means to identify and respond to security incidents, are supporting elements of the Senate Bill.</p> <p>Applies to: All network segments and systems storing, transmitting or processing PII.</p>
FIREWALL MONITORING AND MANAGEMENT	<p>ITGI Key Controls: Requires firewalls and that logs be captured, monitored, and responded to and should be retained at least one year.</p> <p>Applies to: All firewalls, proxies, gateways, and network access control devices.</p>	<p>FFIEC Key Guidelines: Requires firewalls as a core component to network security.</p> <p>Applies to: Network access to segments that transmit, store or process NPI.</p>	<p>HIPAA Key Control: Though a firewall is not specifically required, it is a must-have network security control to protect ePHI.</p> <p>Applies to: Network access to segments that transmit, store or process ePHI.</p>	<p>SB1386 Key Controls: No specific requirements for implementing or maintaining a firewall.</p>
MESSAGING SECURITY AND COMPLIANCE SERVICES ³	<p>ITGI Key Controls: Requires anti-virus as a core requirement for network security.</p> <p>Applies to: All email upon ingress to, and potentially, on egress from corporate networks.</p>	<p>GLBA Key Controls: Anti-virus controls are mentioned in GLBA as is retention of messages.</p> <p>Applies to: Anti-virus applies to all corporate email and retention applies to all email containing NPI data.</p>	<p>HIPAA Key Control: Requires anti-virus. While not specifically stated, the continuity of messaging component could aid in disaster recovery and business continuity required by HIPAA.</p> <p>Applies to: Anti-virus applies to all corporate email and retention applies to all email containing NPI data.</p>	<p>SB1386 Key Controls: No specific requirements for implementing or maintaining email security services.</p>
UNIFIED AUTHENTICATION	<p>ITGI Key Controls: Requires authentication. Two-factor authentication is mentioned as a form of authentication to be evaluated in the context of "common confidentiality requirements.</p> <p>Applies to: Access to any sensitive and/or regulated financial data.</p>	<p>GLBA Key Controls: Requires authentication and access control.</p> <p>Applies to: Authentication methods, access control methods and the administration of access for networks, operating systems, applications, remote users and systems.</p>	<p>HIPAA Key Control: Authentication requirements are fairly broad and do not specify two-factor for access to ePHI.</p> <p>Applies to: Useful for high level of compliance to requirements for remote access/VPN, Web application and security device authentication.</p>	<p>SB1386 Key Controls: While authentication is not addressed specifically, the ability to trace access to personal data is a feature that a strong authentication/identity management solution can provide.</p> <p>Applies to: All systems storing, transmitting or processing personally identifiable information (PII).</p>
MANAGED PUBLIC KEY INFRASTRUCTURE (MPKI) AND SECURE SOCKET LAYER (SSL)	<p>ITGI Key Controls: Requires encryption. Encryption and non-repudiation are both required under the ITGI standards but spoken of very broadly.</p> <p>Applies to: Sensitive and regulated financial data and the systems storing, processing, or transmitting those data.</p>	<p>FFIEC Key Guidelines: Encryption in storage and transmission, and integrity controls.</p> <p>Applies to: All systems storing, transmitting or processing regulated data (Non-public personal information.)</p>	<p>HIPAA Key Controls: Requires encryption of both data at rest and in transmission. MPKI and SSL appear to have the most references in HIPAA particularly as it relates to encryption of PHI, access to PHI, and integrity controls.</p> <p>Applies to: ePHI in storage and in transmission.</p>	<p>SB1386 Key Controls: Though not addressed directly in SB1386, MPKI is very useful for SB1386 compliance.</p> <p>Applies to: PII in storage and in transmission.</p>

COMPLIANCE SOLUTIONS: STANDARDS	PAYMENT CARD INDUSTRY (PCI)	NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL (NERC) URGENT ACTION STANDARD 1300	ISO 17799
CONSULTING ASSESSMENTS	PCI Key Controls: In addition to the annual assessment for level 1 (large) merchants and level 1 and 2 service providers, it requires annual penetration testing and application testing. Applies to: Credit card processing systems.	NERC Key Controls: "Risk-based" assessments must be performed on critical and cyber assets. In addition, an annual Cyber Vulnerability Assessment is required. Applies to: All entities responsible for planning, operating, and using the bulk electric system.	ISO 17799 Key Controls: Requires annual Risk Assessments and initial compliance assessment. Assessments specific to specific ISO domains (10 areas covering all aspects of information security). Applies to: Enterprise or specified environments
HOST LOG FILE MONITORING	ITGI Key Controls: Requires logging for all access to credit card data. Applies to: Credit card processing systems.	NERC Key Controls: Logs must be kept and maintained for 90 days of authorized access and unauthorized access to the security perimeter. Logs must be generated on a 24x7x365 basis and reviewed manually every two months. In addition, records of reviews must be kept. Applies to: All entities responsible for planning, operating, and using the bulk electric system.	ISO 17799 Key Controls: Requires log monitoring and analysis program. Applies to: Enterprise or specified environments.
MANAGED VULNERABILITY PROTECTION SERVICE (MVPS)	PCI Key Controls: Requires quarterly scans and annual penetration tests. For external scans, an approved vendor must be used. Requires alerts. Applies to: Credit card processing systems and network devices.	NERC Key Controls: An annual Cyber Vulnerability Assessment is required, which includes scanning. In addition, the entity must have controls in place to ensure patches are up-to-date. Applies to: All entities responsible for planning, operating, and using the bulk electric system.	ISO 17799 Key Controls: Requires vulnerability scanning and annual penetration tests. Requires alerts. Applies to: Enterprise or specified environments.
INTRUSION DETECTION SERVICE	PCI Key Controls: Requires host and/or network intrusion detection or prevention. Applies to: Credit card transmission networks, processing and storage systems.	NERC Key Controls: 24x7x365 monitoring of the Electronic Perimeter for unauthorized access is required. Applies to: All entities responsible for planning, operating, and using the bulk electric system.	ISO 17799 Key Controls: Requires host and/or network intrusion detection or prevention. Applies to: Enterprise or specified environments.
FIREWALL MONITORING AND MANAGEMENT	PCI Key Controls: Requires an appropriately configured and managed firewall. Applies to: Firewalls providing access to credit card processing and storage systems.	NERC Key Controls: A firewall is required component for a secure electronic perimeter. Applies to: All entities responsible for planning, operating, and using the bulk electric system.	ISO 17799 Key Controls: Requires an appropriately configured and managed firewall. Applies to: Enterprise or specified environments.
MESSAGING SECURITY AND COMPLIANCE SERVICES³	PCI Key Controls: Requires Anti-virus for e-mail security. Applies to: All email upon ingress to and, potentially, on egress from corporate networks.	NERC Key Controls: Antivirus is required and signature files must be updated within 30 days or release. Applies to: All entities responsible for planning, operating, and using the bulk electric system.	ISO 17799 Key Controls: Antivirus is required and signature files must be updated within 30 days or release. Applies to: Enterprise or specified environments.
UNIFIED AUTHENTICATION	PCI Key Controls: Requires two-factor authentication Applies to: Remote access to credit card processing environments.	NERC Key Controls: Strong authentication (to augment user name and passwords) is required for remote access to electric systems. One-time passwords and digital certificates are mentioned as options for strong authentication. Applies to: All entities responsible for planning, operating, and using the bulk electric system.	ISO 17799 Key Controls: Requires Anti-virus for e-mail security. Applies to: Enterprise or specified environments.
MANAGED PUBLIC KEY INFRASTRUCTURE (MPKI) AND SECURE SOCKET LAYER (SSL)	PCI Key Controls: Requires 128-bit SSL encryption and that crypto keys and their transmission and storage be effectively managed. Applies to: Databases, Web servers and applications that store and/or process credit card data.	NERC Key Controls: Strong authentication (to augment user name and passwords) is required for remote access to electric systems. One-time passwords and digital certificates are mentioned as options for strong authentication. SSL encryption is not mentioned in the standard. Applies to: All entities responsible for planning, operating, and using the bulk electric system.	ISO 17799 Key Controls: Requires two-factor authentication for high value assets such as routers, VPN, FWs. Applies to: Enterprise or specified environments.

NOTES

- The IT Governance Institute's (ITGI) document titled "IT Controls for Sarbanes Oxley" was the source for the SOX interpretation.
- FFIEC is the Federal Financial Institution Examination Council. FFIEC audit procedures cover GLBA and most other banking regulations.
- In addition to the regulations noted, the U.S. Securities and Exchange Commission and National Association of Securities Dealers regulations also require certain message archiving and message continuity services.

 Specific Mention	 Implied Relationship at Best
 Limited Mention	 Not Applicable

This document is intended to provide an overview of certain regulations and should not be construed as a legal opinion or an exhaustive examination of all potentially applicable regulations. The services noted above do not ensure compliance but can be important components of an overall compliance strategy.



Service Description: Certification begins with a highly detailed assessment that VeriSign performs. Key tasks include documentation review, interviews, architecture analysis, vulnerability scanning, configuration review, and review of identity and access management. After this extensive review, most companies have a few things to fix; once corrections are remediated, VeriSign performs the final check and issues certification. Certification does not have to be for an entire enterprise. It can be scaled to specific applications, infrastructures, and business units.

Service Features: The outcome of the VeriSign assessment includes a detailed report on VeriSign's findings and recommendations, a certification letter, and the ability to display certification on your company Web site. In addition, VeriSign provides the database of findings so that you can obtain relevant details for specific areas of focus. This is particularly useful in compliance, where mapping internal controls to specific regulations is critical.

Enterprise Risk and Compliance Assessments

Looking for something more focused than broad-based certification, such as for the annual risk assessment required by the Health Insurance Portability and Accountability Act (HIPAA)? What about risk assessments of your business partners?

Bottom Line: Enterprise risk and compliance assessments are essential for understanding your security risk and developing a roadmap for improvement and compliance.

Service Description: VeriSign® Enterprise Risk and Compliance Assessments allow you to perform targeted (or broad-based) risk analysis based on one or more regulations or standards. This includes Payment Card Industry (PCI) assessments, for which VeriSign is a leading provider. A VeriSign assessment is designed to map to the targeted regulations or standards, and includes policy reviews, interviews, architecture analysis, technical assessment, configuration reviews, and other tests. Some companies use proprietary technology that gives the customer a score without explaining what the assessment is based on. VeriSign uses an open-standards based approach, allowing you to see and understand the evaluation and its parameters. In addition, VeriSign's standards-based assessments map to industry standards and regulations.

Service Features: Assessments result in detailed reports and recommendations that map your controls to industry and regulatory requirements. In addition, VeriSign helps you prioritize and plan the activities required to improve your overall security and compliance posture.

Application Security Services

Even with firewalls, intrusion prevention devices, and patched operating systems, vulnerabilities within application code can create new points of entry for hackers. Seventy-five percent of network attacks occur at the application layer (eWeek, *App Developers Need to Redouble Security Efforts*, September 30, 2004.). Attacks aimed at credit card processing, online banking, and other financial systems may have compliance implications because of the sensitive data that is stored and processed. The healthcare and energy industries are at risk too, because of their reliance on distributed applications.

Bottom Line: Best practices and certain regulations and industry standards dictate that you protect your critical applications by addressing security throughout the development and implementation lifecycle.



Service Description: VeriSign offers a variety of services to address application security. They include:

- Software Development Lifecycle (SDLC) security analysis and development
- Security education, awareness, and training for developers
- Application architecture review and design
- Application penetration testing for both Web applications and non-Web applications
- Application code review and analysis
- Application certification, including the PCI Assessment Services as well as the VeriSign® Security Certification Program

VeriSign® Application Security Services help address the following aspects of some key regulations and standards:

- The Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA), and Health Information Portability and Accountability Act (HIPAA), which all require the integration of security into the SDLC
- The Payment Card Industry (PCI) Data Security Standard (DSS), which now includes application testing in its scanning requirements; and the Payment Application Best Practices standard, which is published by the PCI, but is not mandatory
- Industry standards from the Open Web Application Security Project (OWASP) and the Web Application Security Consortium (WASC), which have gained significant traction and are often looked to for guidance when conducting application testing

Service Features: VeriSign provides a detailed report that maps findings and recommendations to the standards being used for assessment (e.g., OWASP, WASC, or PCI).

Security Program Development

The majority of key regulations and standards require organizations to have a formal security policy, well-defined standards and procedures, dedicated security personnel, and security awareness activities.

Bottom Line: Companies and government agencies cannot meet compliance requirements without a formal information security program.

Service Description: VeriSign Security Program Development Services help companies develop sound security programs. From policy development to security awareness and training, VeriSign's skilled professionals can help you improve your security program, posture, and compliance. If you need to jump-start or augment your security program, VeriSign can also provide interim or strategic staffing for senior positions such as an interim chief information security officer (CISO).

Service Features: VeriSign® Security Program Development Services produce tangible deliverables such as policies, procedures, and training materials. VeriSign's seasoned practitioners, who average ten years hands-on experience in information security, complement your information security team by coming up to speed quickly and working closely with existing staff to produce long-term solutions.



VeriSign® Managed Security Services

Although a solid security program and regular assessments provide a good foundation for compliance, you must monitor your security posture on an ongoing basis to meet key compliance requirements. Performing a battery of monitoring activities 24/7 can be a tedious, resource-intensive process that distracts in-house personnel from core, value-producing activities. Enter VeriSign® Managed Security Services (MSS), which provides levels of security management and monitoring that may be too expensive or too resource-intensive to perform internally.

Host Log Monitoring

The ability to log, track, and analyze user and system activity is often critical for preventing, detecting, responding to, and remediating security breaches. It is also a key requirement for compliance with a number of standards and regulations.

Bottom Line: Compliance can depend on the oversight and control of assets that maintain sensitive data.

Service Description: VeriSign® Managed Host Log Monitoring Service collects critical event data where it is most detailed, at the host. The service securely collects your logs and monitors them for suspicious activity as well as key events that are important from a security and compliance perspective.

Managed Host Log Monitoring Service helps address the following aspects of some key regulations and standards:

- Logging requirements for Sarbanes-Oxley (from the IT Governance Institute's (ITGI) IT Controls for Sarbanes-Oxley Framework)
- PCI requirement 10.2 requiring "automated audit trails" for access to credit card data
- North American Electric Reliability Council (NERC) requirements for monitoring electronic access control
- HIPAA and GLBA requirements for logging access to personal information
- ISO 17799 section 10.10, "Monitoring"

Service Features: Managed Host Log Monitoring Service automatically alerts you to critical events. Authorized personnel can access logs and reports 24/7 via VeriSign's secure MSS Portal, and can also customize reports to view activity by source, event, and so on.

Intrusion Detection and Prevention

Hackers continually search for vulnerabilities and new ways to compromise networks. As the complexity and scope of network threats grows, simply installing network security technology does not guarantee protection or compliance. In many cases, it simply leads to a false sense of security.

Bottom Line: An organization must be able to detect and prevent intrusions. Doing so requires vigilant 24/7 monitoring.

Service Description: VeriSign® Managed Intrusion Detection and Prevention Services provide full management and 24/7 monitoring of your intrusion detection system (IDS) and intrusion prevention system (IPS) devices. VeriSign remotely manages and supports many of the leading network- and host-based IDS and IPS technologies. VeriSign also offers an open-source (i.e., Snort) network intrusion detection installation for companies wanting to minimize capital investment. VeriSign handles signature updates and configuration management, and alerts you only to events that threaten your infrastructure.



Managed Intrusion Detection and Prevention Services support the following regulations and standards:

- PCI requirement 11.4 requiring intrusion detection monitoring
- Federal Financial Institutions Examination Council (FFIEC) guidelines for GLBA
- NERC requirements for monitoring electronic access control
- ISO 17799 sections 10.6, “Network Security Management,” and 10.10, “Monitoring”

Service Features: The service automatically alerts you to critical events. Authorized personnel can access IDS and IPS events and reports 24/7 via VeriSign’s secure MSS Portal.

Firewall Management and Monitoring

Most organizations today have firewall technology, yet viruses and unauthorized access continue to plague them. Insufficient firewall monitoring, system reconfiguration oversights, and other weaknesses contribute to firewall vulnerabilities.

Bottom Line: No matter what regulations and standards you are subject to, firewalls—and effective management of them—are critical components of network security.

Service Description: VeriSign® Managed Firewall Service offers comprehensive firewall management. It includes upgrades, configuration management, rule-set changes, and health monitoring. In short, VeriSign can manage your firewalls cost effectively while you focus on your core business.

Managed Firewall Service helps address the following aspects of some key regulations and standards:

- Logging/monitoring requirements for Sarbanes-Oxley (from the ITGI’s IT Controls for Sarbanes-Oxley Framework)
- PCI requirement 1 requiring companies to install and maintain a working firewall
- FFIEC guidelines for GLBA
- NERC requirements for electronic security perimeter assessments
- ISO 17799 sections 10.6, “Network Security Management,” 10.10, “Monitoring,” and 11.4, “Network Access Control”

Service Features: Reports and statistics are available 24/7 via VeriSign’s secure MSS Portal.

Managed Vulnerability Protection

Depending on the standard or regulation, scanning and assessment requirements may apply not only to network and operating systems, but also to externally facing applications that cannot be sufficiently assessed using automated technology alone.

Bottom Line: Vulnerability protection and ongoing scanning is either explicit or implicit within most key regulation and requirement. Furthermore, it is essential for protecting your network from threats of attack.



Service Description: VeriSign® Managed Vulnerability Protection Services provide regular scanning and assessment of your critical infrastructure. Manual testing by experienced professionals is combined with automated technology to help identify the breadth and depth of vulnerabilities. Most important, this is not simply an automated scanning service. VeriSign’s team communicates regularly with you to discuss findings and recommendations for further improvement, and to keep you up to date on the latest vulnerabilities and threats. VeriSign is also an approved provider for quarterly PCI scanning.

Managed Vulnerability Protection Services helps address the following aspects of key regulations and standards:

- Sarbanes-Oxley requirements for regular assessment of network and application vulnerabilities (from the ITGI’s IT Controls for Sarbanes-Oxley Framework)
- PCI requirements for quarterly scanning
- HIPAA and GLBA requirements for regular assessment
- NERC requirements for electronic security perimeter assessments
- ISO 17799 sections 12.6, “Technical Vulnerability Management,” and 15.2.2, “Technical Compliance Checking”

Service Features: Managed Vulnerability Protection Services tailors scanning and assessment intervals to your requirements. VeriSign’s secure MSS Portal maintains all the collected vulnerability findings, trends, and recommendations. It also maintains workflow information so that you can use the portal 24/7 to track and manage your vulnerability posture.

VeriSign® Unified Authentication

Although password-based authentication is one of the easiest authentication methods to implement, it is also the least secure, because passwords and PINs can be easily shared, stolen, or guessed. By requiring users to present something they know (e.g., a user name/password or PIN) with something they have (e.g., a token, digital certificate, or smart card), strong authentication helps organizations more accurately identify users and devices accessing the network.

Bottom Line: Strong (two-factor) authentication is specifically required by several regulations; besides, it’s just good security practice.

Service Description: Digital certificates and public key infrastructure (PKI) were the first managed services provided by VeriSign, which now provides best-of-breed strong authentication solutions via VeriSign® Unified Authentication. Whether your company needs one-time-passwords or traditional PKI, VeriSign can help meet your requirements cost effectively—and without deploying additional infrastructure. VeriSign leverages your existing architecture (e.g., Windows Active Directory or Lightweight Directory Access Protocol (LDAP)) and can also provide both an in premise or “in-the-cloud” validation deployment model to meet your needs. Unified Authentication is the most comprehensive strong authentication solution, offering a wide choice of credentials, devices, and deployment options for securing world-class global enterprises.



VeriSign Unified Authentication provides:

- More value: Unified Authentication delivers more value with OTP tokens on a single integrated platform.
- Less cost: Enterprises gain up to 40% lower TCO with cost-effective tokens without adding new infrastructure and by deploying user self-service applications. Unified Authentication leverages investments in existing infrastructures, including the central user directory, user provision and SSO middleware, AAA servers and administration tools, enabling an easily integrated and deployed solution.
- A system that is designed to fit: Provides maximum deployment flexibility with the option of using an in-the-cloud validation utility or an in-premise validation engine for those enterprises that require more control of the overall infrastructure
- A solution that is future proof: VeriSign Authentication offers an open solution based on the standards defined by OATH, an industry wide working group for strong authentication, as opposed to a proprietary one which ensures constant innovation and reduced costs.

VeriSign Unified Authentication helps address the following aspects of some key regulations and standards:

- PCI requirement 8.3 for two-factor authentication for remote access
- GLBA (Gramm-Leach Bliley Act) requirements for authentication and access control
- FFIEC requirements for access control to personal information
- NERC requirements for strong authentication when accessing power systems remotely
- ISO 17799 section 11.4, “Network Access Control”

Service Features: VeriSign strong authentication credentials can be used on enterprise desktops or externally via a VeriSign token that allows users to conveniently carry security credentials with them. In addition, you can provision and manage all types of authentication credentials from a single platform.

VeriSign® Messaging Security and Compliance Services

Several key regulations such as the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX), and agencies such as Securities and Exchange Commission (SEC), and the National Association of Securities Dealers (NASD), have imposed strict requirements for documentation, retention, transparency, and protection of electronic communications. To comply with these regulations, organizations must place physical and procedural safeguards on all electronic data that they transmit or store, and they must protect and monitor all communications.

Bottom line: Message security, archiving, and continuity are critical for compliance.

Service Description: VeriSign® Messaging Security and Compliance Services provide a broad range of offerings related to email messaging:

- Message Archive Service – Provides retention, retrieval, indexing, and archiving of email.
- Message Continuity Service – Provides email continuity and disaster recovery. The service maintains copies of all inbound and outbound emails in a 30-day message store, allowing you to recover quickly should your email system go down.
- Email Security Service – Provides a hosted anti-virus and spam filtering service.



VeriSign Messaging Security and Compliance Services helps address the following aspects of some key regulations and standards:

- HIPAA requirements for message archiving, confidentiality, and highly available email
- GLBA requirements for protecting and maintaining email that contains non-public personal information
- Sarbanes-Oxley requirements to retain certain email correspondence for at least five years
- SEC Rule 17A-4 and NASD Rules 3010 and 3110, which require organizations to retain certain correspondence for at least five years

Service Features: VeriSign Message Security and Compliance Services offer a fully outsourced solution. A secure portal gives you 24/7 access to reporting, email, and other management features.

+ The VeriSign Difference

Many companies offer a “silver bullet” approach to compliance, addressing regulations and standards piecemeal and with proprietary technology that does not scale easily to meet changing requirements. At VeriSign we know better. Our services have always mapped to the building blocks and critical activities of a comprehensive information security program. It is no surprise that the regulations and industry standards map back to the same set of best practices that VeriSign supports. While we actively monitor new regulations and have adjusted our offerings to reflect specific reporting and retention requirements, the core services themselves have not changed.

VeriSign believes that helping companies meet compliance requirements involves understanding a rapidly changing landscape, identifying the activities that go into building and maintaining a compliance infrastructure, and providing services that map to those activities. That is our core expertise; that is how we help you.

+ For More Information

For more information about VeriSign® Compliance Solutions, please call 650-426-5310 or email enterprise_security@verisign.com.

+ About VeriSign

VeriSign, Inc. (Nasdaq: VRSN), delivers intelligent infrastructure services that make the Internet and telecommunications networks more intelligent, reliable, and secure. Every day VeriSign helps thousands of businesses and millions of consumers connect, communicate, and transact with confidence. Additional news and information about the company is available at www.verisign.com.

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

© 2005 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, “Where it all comes together,” 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. All other trademarks are the properties of their respective owners.

00021327 10-27-05