



**SOLUTION
OVERVIEW**



VeriSign® Global Security Consulting



Where it all comes together.™



CONTENTS

| | |
|--|----|
| + Introduction | 3 |
| + Global Security Consulting | 4 |
| VeriSign® Security Certification Program | 4 |
| Enterprise Risk and Compliance Assessments | 4 |
| Technical Security Assessments | 6 |
| Security Policy and Program Services | 8 |
| Security Architecture and Design | 9 |
| Identity and Access Management | 10 |
| Incident Response and Forensics | 10 |
| Disaster Recovery and Business Continuity | 11 |
| Security Technology Integration | 11 |
| + Our Industries | 12 |
| + Our Expertise | 13 |
| + The VeriSign Difference: Expertise, Intelligence, Trust | 13 |
| + Learn More | 14 |
| + About VeriSign | 14 |



VeriSign® Global Security Consulting

+ Introduction

The mission of VeriSign® Global Security Consulting (GSC) is to blend unmatched security expertise with world-class business and program management in order to provide comprehensive enterprise security solutions to our clients. Our experts combine business-driven approaches with technology expertise in order to deliver maximum client satisfaction. VeriSign security consultants average 10 years of experience. They are professionals who have actually experienced real-world security and compliance implementations. Many of our practitioners have worked in the financial industry, commercial enterprises, and the government.

Because many of the challenges that businesses face today are as much organizational as they are technical, a resilient infrastructure alone is not enough. VeriSign works to improve security and compliance policies and practices, business processes, and the organization's understanding and observance of such. We do not recommend technical improvements without also considering the organizational changes required to make them effective.

At VeriSign, we do not create our own proprietary set of standards. We use standards and control requirements that are both generally accepted as industry practices and are often required to be adhered to by government or industry regulation. Most important, our expertise across these standards allows us to provide holistic security solutions that map to these many diverse requirements in a cost-effective manner. Our work is built on the solid foundation of frameworks such as ISO 17799, the Information Security Forum (ISF) Standard of Good Practice, Control Objectives for Information and Related Technology® (COBIT), and Basel II. Key standards and regulations include, but are not limited to:

- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Sarbanes-Oxley Act (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- California Security Breach Notice Act (formerly Senate Bill 1386) and other state notification statutes
- Federal Information Security Management Act (FISMA)
- Presidential Homeland Security Directives and other federal and state regulations and requirements
- Federal Financial Institutions Examination Council (FFIEC)
- Various frameworks for public company Sarbanes-Oxley Section 404 compliance, including the IT Governance Institute® and the Information Systems Audit and Control Association (ISACA)
- Payment Card Industry (PCI) Data Security Standard (formally Visa CISP and MasterCard SDP)
- Industry-specific standards such as BITS Financial Services Roundtable and North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) Standards 002 through 009 (CIP-002 through CIP-009)

Finally, GSC serves the largest companies and government agencies in the world. Our depth of intelligence and broad customer base allows us to easily compare organizations in similar business or regulatory environments.



+ Global Security Consulting Services

VeriSign® Security Certification Program

The VeriSign Security Certification Program is the flagship offering of the VeriSign suite of compliance solutions. It bridges our offerings from Global Security Consulting, VeriSign® Managed Security Services (MSS), and VeriSign® Unified Authentication (UA). Where the consulting organization provides the assessment and certification, our MSS and UA services provide a cost-effective means to managing the myriad of required ongoing security activities.

This premium service is designed to assess an enterprise's information security program (or critical business component or application) and certify that it meets standards for best practices. In turn, it provides trust and assurance for companies that are required to communicate their security practices and posture to third parties and government regulators, and can reduce the complexity and expense of multiple audits.

The comprehensive assessment can focus on an environment from an enterprise, strategic business unit, technology infrastructure, or critical application perspective.

- People, policies, and practices assessments
- Internal and external network and security architecture reviews
- Technical risk assessments
- Vulnerability scanning
- Device configuration reviews
- User access and account reviews

Upon completion of the assessment, the organization receives a comprehensive report that includes VeriSign findings and recommendations. If in VeriSign's professional judgment and in accordance with the agreed-upon standards, the organization adequately meets the standards in the VeriSign Security Certification Program requirements, then it is certified.



The certification can be used to communicate security practices to clients, business partners, regulators, and other third parties. In addition, as compliance is never a point-in-time activity, we work with our clients to ensure that the organization is doing the ongoing activities that help maintain their overall security posture.

Enterprise Risk and Compliance Assessments

VeriSign® Enterprise Risk and Compliance Assessments provide detailed analysis of an organization based on the following five areas:

- Security policy and processes
- Security/privacy program management
- Technology infrastructure and security controls
- Security organization and governance
- Operational effectiveness



In-depth evaluation of these key areas enables VeriSign to describe an organization's overall security objectives and assess its current ability to support them. Keeping pace with the dynamic security threats facing an organization, the assessment compares each area to the evolving vulnerabilities and business risks that are relevant to each specific client.

As a result, VeriSign identifies the strengths and weaknesses of its clients, and recommends practical measures to align a security program with their business objectives. This helps clients prioritize spending for the highest-value and highest-risk security and privacy efforts, track changes in their security program and provide a long-term perspective on its effectiveness, and improve the accuracy of due diligence efforts during a merger, acquisition, or strategic partnership.

In addition to enterprise-wide assessments, VeriSign also offers focused compliance assessments against key regulations and standards. These assessments include:

- **Payment Card Industry (PCI) data security assessments** – As one of the first Visa and MasterCard approved assessors, VeriSign has performed hundreds of PCI security assessments for large merchants, service providers, and financial institutions. VeriSign has more than 40 PCI-certified assessors.
- **IT Controls for Sarbanes-Oxley** – Although VeriSign is not an auditing firm, we frequently help clients in the gap analysis, design, and implementation of IT security controls that help them meet the requirements for Sarbanes-Oxley.
- **Public-sector Certification and Accreditation (C&A)** – VeriSign helps government agencies address requirements needed to attain certification that covers applicable government regulations, including OBM A-130 and DoD Information Technology Security Certification and Accreditation Process (DITSCAP).
- **HIPAA** – VeriSign has performed numerous risk assessments for HIPAA. We also help companies design infrastructures and controls that support the HIPAA requirements and help them protect personal health information.
- **Gramm-Leach-Bliley (GLBA)** – VeriSign performs focused assessments for GLBA-governed financial institutions. These assessments are typically designed to help companies meet the necessary IT security requirements for upcoming FFIEC or Federal Trade Commission (FTC) audits.
- **North American Electric Reliability Council (NERC)** – VeriSign performs focused assessments for the energy industry around NERC standards CIP-002 through CIP-009.
- **Notification statutes** – Although California's Security Breach Notice Act was the first, many states now have notification statutes. This focused assessment helps companies ensure they have the necessary notification procedures in place and that they address any additional or compensating controls, such as encryption.

In addition to the above regulatory-focused assessments, GSC often performs cross-regulatory assessments on key areas of concern such as policies, encryption, incident response and notification, logging, access control, and authentication.



Technical Security Assessments

VeriSign's technical security assessments encompass all layers of an organization's architecture. This includes analysis to identify vulnerabilities in network, host, database, application, and wireless infrastructures.

Network Vulnerability Assessment and Penetration Testing

VeriSign's network vulnerability assessments and penetration testing identify network vulnerabilities using the most sophisticated techniques available. Mimicking a malicious intruder, VeriSign gathers network information, runs automated scanning tools, and uses extensive manual testing to discover network vulnerabilities. VeriSign's external network vulnerability testing probes Internet points-of-presence for known security vulnerabilities. Internal network vulnerability testing assesses network security from inside a DMZ or from within an organization. At the customer's request, we can also attempt to penetrate the systems that we are evaluating. All testing uses strict controls with an emphasis on protecting each customer's security and privacy.

Application Security Assessment

VeriSign's application security assessments identify security vulnerabilities by reviewing and probing an application's security controls. This "black box" security testing examines an application's run-time behavior using a variety of techniques customized for each application type.

Examples of application security assessment tests include:

- Testing the capability to replay authentication data
- Looking for exposure of sensitive data on servers
- Attempting to exploit encryption algorithms
- Taking advantage of inadequate input validation controls

Tests are performed both from the perspective of a trusted user and as an anonymous user (without valid user credentials). VeriSign incorporates standards and best practices from sources such as the Open Web Application Security Project (OWASP) and the Payment Card Industry's Payment Application Best Practices. A detailed findings report, including a prioritized issues list and recommendations for remediation of discovered vulnerabilities, is provided

Application Code Review

VeriSign's application code review service is one of VeriSign's most in-depth security assessments. Starting with an application security architecture review, VeriSign analyzes the application's source code from the perspective of a developer looking for design flaws, programming flaws, and the use of vulnerable functions or programming constructs. Any one of these weaknesses can be buried in thousands or millions of lines of application code, and VeriSign performs the arduous task of finding these flaws. VeriSign then details its findings in a clear, concise, and actionable report.

Database Vulnerability Assessment

Given the recent compromises of credit card and personal financial data, database security has become more important than ever. VeriSign performs focused assessments of databases using automated tools and manual techniques in order to assess the security configurations and settings for the database as well as the access controls and rights/permissions.



VeriSign assesses the existing database configurations by comparing the system configuration against standards of good practice.

The following areas are typically assessed:

- User management
- System defaults
- Policies and procedures
- Authentication methods
- Use of encryption
- System and object privileges
- Operating system datafile information
- Operating system roles (if applicable)
- Profiles
- Database roles
- Distributed database features
- Auditing
- Backup/recovery
- Parameter files

After completing this configuration analysis, VeriSign develops recommendations for securing the database that will cover identified vulnerabilities. These recommendations are prioritized for relative risk and level of effort to mitigate.

Wireless Security Assessment

VeriSign's wireless security assessments help clients identify and mitigate risks and vulnerabilities associated with their wireless networks.

This business-focused service includes the following elements:

- Review of the underlying requirements for wireless networks
- Review of the wireless network architecture, configurations, and standards, as well as a detailed review of an organization's wireless deployment strategies, policies, and procedures
- Identification of signal leakage and deployment of unauthorized access points in the enterprise, along with the identification of vulnerabilities in access points and wireless LAN clients
- Appropriate use of encryption technologies to minimize leakage of clear text information

VeriSign details findings in a report that offers a risk-level classification and impact analysis for deploying wireless LAN technology, including the development of "what if" scenarios to assess the impact of a security compromise. VeriSign also includes recommendations to mitigate risks and vulnerabilities associated with an existing wireless LAN infrastructure.



Security Policy and Program Services

VeriSign's security policy and program services can help an organization develop, improve, or communicate security and privacy strategy. VeriSign's team of Certified Information Systems Security Professionals (CISSP®) augments a customer's internal security and privacy staff with on-demand subject matter experts to help align security and organizational strategies with their organization's policies, architectures, and technologies.

VeriSign security policy and program services include:

- Policy and standards review and development
- Program review and development
- Training and awareness
- Interim chief information security officer (CISO) and chief privacy officer (CPO)
- Incident response program development

Policy and Standards Review and Development

VeriSign evaluates the effectiveness of an organization's existing security policies and standards by comparing them against business requirements, current security practices, and industry standards of good practice. Based on VeriSign's findings, we work with our customers to improve their security policies and standards, to meet industry requirements, and to fulfill business objectives.

Program Review and Development

Security programs are composed of business and technology initiatives, as well as market, regulatory, and risk forces. The dynamic nature of these programs means that organizations need an effective strategic planning process. VeriSign's program review and development services provide expert security and business guidance to help organizations reduce the total cost of security and privacy programs.

This service includes:

- Development of practical responses to security and privacy challenges
- Prioritization of near- and long-term security strategies and objectives
- Effective communication of strategic decisions by creating or modifying organizational policies

The result of these services is a well-functioning security and privacy management program across an organization or business unit.

Security Education, Training, and Awareness

It is a well accepted principle in the information security industry that regular training and awareness-building are essential elements to an effective security and privacy program. Employees must understand each program's requirements and how they are expected to comply. Similarly, employees who are unaware of the risks associated with their actions may not fully understand the need for compliance with the policies designed to reduce organizational risk. VeriSign's security education, training, and awareness services address organizational "soft" spots by targeting all stakeholders, from security/privacy experts to management and employees.

VeriSign employs a "train the trainer" strategy and develops custom Training and Awareness workshops. Training for the broader user population covers topics such as passwords, acceptable Internet use, and other matters of importance to the organization. VeriSign also provides specialized training on regulatory compliance issues (HIPAA, GLBA, PCI DSS, European Union Safe Harbor, and so on) and technical areas, such as virtual private networks (VPNs), intrusion detection systems (IDS), and incident management and forensics.



Interim (or Deputy) CISO and CPO

With security and privacy functions gaining increased visibility coupled with a shortage of qualified candidates, it can be difficult to find senior security and privacy personnel such as chief information security officers and chief privacy officers. The VeriSign Interim CISO and CPO program provides organizations with security and privacy experts who become part of the customer's organization to help them address long-term needs.

By providing senior security and privacy staff, VeriSign can help:

- Define the CISO or CPO functions
- Jump-start stalled security or privacy efforts
- Maintain momentum in existing programs during a permanent CISO or CPO search

Incident Response Program Development

As organizations rely more heavily on their digital assets, threats to those assets are on the rise, making it more important than ever to prepare for information security incidents before they occur. VeriSign's incident response program development services assist in the creation, implementation, and rollout of such programs. VeriSign helps its customers create policies and processes to ensure that security incidents are dealt with quickly and effectively. VeriSign creates methodologies to evaluate, mitigate, escalate, and contain incidents in a systematic manner. We also train customer staff to ensure their preparedness for potential incidents. In addition, should the organization require immediate support, we have incident response and computer forensic experts on staff to assist (see below).

Security Architecture and Design

Good network security starts with a resilient architecture as an organization's infrastructure must be designed to minimize the risk of attacks. And, if an attack occurs, the architecture must be built to help contain and recover from it and maintain business operations. To help meet these ends, we look at the architecture and design to pinpoint how the company can improve them. Architecture should be a strategic part of an organization that supports not just immediate goals but the overall business strategy.

For design, or assessment of design, which is often more tactical, VeriSign focuses on identifying the technology that is available to solve the problems at hand. Technology, of course, changes—often rapidly. As such, we re-examine the design frequently to make sure it is up to date. Specifically, the VeriSign team reviews the environment to ensure that the architecture integrates with the policies and procedures discovered earlier. We work with the network and security architects to get a complete understanding of the customer network environment and make recommendations that enable the organization's network security architecture to meet industry best practices.

Review of the network architecture potentially includes the following elements:

- DMZ configurations
- Location of available services (VPN, RAS, proxies, etc.)
- Use of VLAN's
- Presence of firewalls and other filtering devices
- IDS infrastructure
- Network segmentation
- Planned architecture modifications and improvements



Like other assessments, the results of an in-depth architecture analysis will be a report that details the findings and recommendations. In addition, VeriSign consultants also typically develop ideal states (or blueprints for the architecture) followed by a roadmap that presents the components, requirements, and resources required to develop and implement the ideal-state infrastructure. As owner of the .com and .net Domain Name System (DNS), critical infrastructure is a core competency for VeriSign.

Identity and Access Management

Identity management provides an easy and efficient way to create and manage user IDs and user accounts. But identity management itself is limited as it focuses only on the user. VeriSign leads the industry in identity and access management services. We promote the notion of access management—tying together users, information, and physical facilities to make sure that only authorized users have access to critical organizational assets.

We start by evaluating the interdependencies and impediments in the organization such as the regulatory requirements, existing strategies, current processes, and current technical architecture.

This includes an evaluation of:

- Directory and database services
- Applications and associated interfaces
- Operating systems and network architecture

The result of our analysis is the development of an identity and access management strategy. Specifically, we draft a roadmap to help guide current and future activities along with a detailed integration plan. Within this, we identify the solutions that will help address the challenges identified by the organization, such as strong credentialing (or strong authentication), single sign-on (SSO) technology, secure electronic transactions, electronic signatures, and role- or rule-based access control. We rank our recommendations by how effectively they improve processes and advance business goals. We also rate each recommendation by its cost-effectiveness and ease of implementation.

Incident Response and Forensics

VeriSign's incident response and forensics services use the combined skills of the company's forensic specialists, security architects, research and development team, and 24/7 MSS operations to handle the needs of any information security investigation. For incident response, we can provide onsite assessment, forensics, and remediation services should the organization experience some sort of network-based attack. For several of the large Internet-facing worms, VeriSign has deployed a team and/or subject matter expert to serve as the incident manager to oversee and drive containment and recovery activities.

VeriSign also offers more traditional computer forensic services that include investigative services for theft of intellectual property, fraud, employee harassment, or inappropriate use of network resources. For this, VeriSign identifies, gathers, and preserves the electronic evidence needed to take appropriate internal or legal action. VeriSign also provides expert-witness consulting services for companies involved in all types of legal and adversarial proceedings, including assistance with identifying and locating digital evidence relevant to an investigation. More technical services include forensic media analysis, data mining, network monitoring, and digital intelligence services.



Disaster Recovery and Business Continuity

Depending on a company's business and given the potential for lost revenue, lost productivity, lost sales opportunities, inventory spoilage, litigation, and so on—the cost of downtime can range from the thousands to hundreds of thousands of dollars an hour. Given the large costs of disasters, it's possible that one major outage could be devastating. In addition, certain regulations and industry standards, such as the FFIEC, require a recovery and continuity plan. Without an up-to-date plan, the company might be out of compliance.

For an application or Internet service provider, 99.999 percent availability may be required just to remain competitive and protect the brand value. Disaster planning helps keep the company competitive. Finally, protecting profits and the capability to do business is, of course, essential—but protecting employees is paramount.

VeriSign's disaster recovery and business continuity solutions include:

- Assessing an organization's (or business unit's) current disaster recovery plan
- Creating a detailed technical infrastructure strategy to implement current plans
- Development of business continuity and disaster recovery plans
- Creating implementation plans for the technical architecture that the plan requires (including cold, hot, and warm sites)
- Providing education, training, and awareness services

Security Technology Integration

VeriSign's security technology integration services provide “hands-on” assistance for the more challenging areas in information security.

Customized to each customer's unique requirements, VeriSign integration services include:

- Security technology analysis and integration
- Secure application engineering support
- IDS engineering and support
- Log monitoring and security event management support

These services can be aligned with VeriSign Managed Security Services to help organizations develop a comprehensive solution to a business security problem using a combination of design and outsourced services.

Security Technology Analysis and Integration

With accelerated technological change and shortened application development cycles, security and privacy staff is faced with the challenge of understanding and evaluating an expanding array of new and updated applications, services, and technologies. VeriSign's security technology analysis and integration services help organizations assess critical IT infrastructure elements and then determine the proper installation, configuration, and “security-hardening” procedures for each system. VeriSign also provides an unbiased security perspective when evaluating or deploying new technologies, such as wireless infrastructures, directory services, e-commerce applications, and other leading technology. Through the VeriSign® iDefense Security Intelligence Services, VeriSign consultants have early access to information and training in new technologies and are updated (in real time) on the latest vulnerabilities. This information helps shorten the deployment cycle of new technology into client organizations.



Secure Application Engineering Support

VeriSign's secure application engineering support services allow VeriSign consultants to assist a customer's internal team throughout the entire application development lifecycle. VeriSign works in all phases of high-level and technical design, product/technology selection, implementation testing, deployment, and performance tuning. This comprehensive engineering support ensures that the correct security controls are adequately addressed in the application design and development process, instead of being retrofitted at a later time resulting in much higher budget and resource costs.

IDS Engineering and Support

VeriSign's IDS engineering and support services draw on VeriSign® Intrusion Detection Management Service expertise to help organizations design, deploy, and tune IDS implementations. VeriSign educates customers on the proper review process for alerts and assists with IDS training and response planning. On an as-needed basis, VeriSign reviews reports with customers and supplies organizations with a list of high, medium, and low threats as they arise. VeriSign can also simulate attacks to test and validate a customer's IDS technology and response capability.

Log Monitoring and Security Event Management Support

Effective security event management is by no means a small undertaking and is much more complex than merely procuring security event management technology. VeriSign consultants have designed log monitoring and event management infrastructures for our large, often regulated, customers.

We provide a comprehensive solution that includes:

- Identifying monitoring needs through an evaluation of necessary regulations, standards, and business requirements
- Identifying and evaluating necessary technology (or services) to gather and analyze the necessary information
- Developing the necessary analytical and response processes to ensure that not only is data being captured and analyzed, but also the results are reviewed on a regular basis and appropriate notification occurs
- Developing unique or custom log/event monitoring signatures for key operating platforms and critical applications
- Providing ongoing support for tuning and implementation of the solutions
- VeriSign feels very strongly that this strategic component is necessary for effective security event monitoring. Whether the organization is planning on using VeriSign® Host Log Monitoring Service or an in-house product, this undertaking is critical.

+ Our Industries

We serve all major industries but tend to focus on those that are either regulated or use security as a competitive differentiator. Key industries include:

- Fortune 1000
- Financial institutions
- Telecommunications
- Healthcare and life sciences
- Retail
- Manufacturing
- Technology
- Public sector
- Utilities



+ Our Expertise

Our consultants average nearly ten years of experience. Some of them have more than 20 years of experience and have worked in a variety of environments, from corporate IT and security to technology, development, and professional services in all the industries we support.

Almost all our consultants have at least one certification and more than 90 percent are CISSPs. The following table lists some of the certifications earned.

| | |
|---------|--|
| CISA | Certified Information Systems Auditor |
| CISM | Certified Information Security Manager |
| CPA | Certified Public Accountant |
| CFE | Certified Fraud Examiner |
| GCFA | GIAC Certified Forensic Analyst |
| GCFW | GIAC Certified Firewall Engineer |
| GCIAC | GIAC Certified Intrusion Analyst |
| GCWN | GIAC Certified Windows Engineer |
| SSCP | Systems Security Certified Professional |
| CCSA | Check Point® Certified Security Analyst |
| CCSE | Check Point Certified Security Engineer |
| IAM NSA | InfoSec Assessment Methodology |
| S+ | S+ Security Plus |
| PMP | Project Management Professional |
| Other | Microsoft and Cisco systems and network certifications |

Our consultants engage in ongoing training and development to maintain a high level of proficiency. Several of our consultants have been involved in the development of computer security programs—both undergraduate and graduate—at colleges and universities. Our consultants hold leadership positions with the Information Systems Security Association (ISSA®) and the Information Systems Audit and Control Association (ISACA) and are active participants in industry associations and consortiums.

+ The VeriSign Difference: Expertise, Intelligence, Trust

Few companies match VeriSign’s experience and expertise, depth and breadth of services, robust infrastructure, intelligence, and role as trusted advisor. VeriSign® Security Services leverage exceptional knowledge, training, and experience; best-of-breed solutions; a global network of proven technology; and VeriSign’s history of stability and trust to deliver cost-effective solutions for proactively managing information security risk.

The following characteristics distinguish and differentiate VeriSign offerings:

- **Global scale and intelligent infrastructure** – With a worldwide customer base and thousands of security devices under management, VeriSign has the scale to support the largest and most demanding organizations and the flexibility to support smaller enterprises where security is also a concern. The breadth of devices that VeriSign monitors affords the company a wider and deeper view of Internet activity. It leverages this unique threat intelligence, as well as the intelligence gathered by the VeriSign iDefense® Security Intelligence Services team to proactively identify—and alert customers to—emerging attack trends and cyber threats.



- **Seasoned practitioners** – With an average of more than ten years' experience in enterprise information security and three or more industry certifications per consultant, the VeriSign consulting team boasts one of the highest concentrations of credentialed experts in the industry. 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 the unique requirements of its business, but also receives prompt attention when security events or other issues arise.
- **World-class support for industry-leading technology** – 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 security solutions that meet the specific requirements of its customers and maximize the effectiveness of their existing security investments.
- **Trusted partner** – VeriSign has a strong heritage in providing trusted security services, and thousands of organizations benefit from this heritage every day. Together with strong authentication, security consulting, threat intelligence, and e-commerce security, VeriSign Managed Security Services represent an unparalleled commitment to helping enterprises engage confidently in electronic commerce, communications, and collaboration.

+ Learn More

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

+ About VeriSign

VeriSign, Inc. (Nasdaq: VRSN) operates intelligent infrastructure services that enable and protect billions of interactions everyday across the world's voice and data networks. Additional news and information about the company is available at www.verisign.com.

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

©2006 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. Check Point is a trademark of Check Point Software Technologies Ltd. CISSP is a registered certification mark of ISC2. COBIT is a registered trademark of the IT Governance Institute. ISSA is a registered trademark of the Information Systems Security Association, Inc. All other trademarks are the properties of their respective owners.

00017413 08-09-06