

M VIRTUALIZATION ECONOMICS DISCOVER INNOVATE RELIAB
NFORMATION GLOBAL CHANGE INTELLIGENT TECHNOLOGY SI
GHT OPPORTUNITY SOCIAL INFRASTRUCTURE INTEGRATE ANA

Security Services From Hitachi Data Systems

Securely Pursue Business Objectives, Manage Risk and Meet Compliance Frameworks

Security Services from Hitachi Data Systems address your business priorities with:

- Information security consulting services that encompass governance, risk and compliance functions.
- A team of security experts with industry certifications and real-life experience as security practitioners.
- An approach that relates business objectives to the protection of information and information systems.

Security Challenges and Industry Trends

World news and major security surveys confirm that cyber threats are growing in size, severity and sophistication. Successful data breaches in high-profile U.S. corporations alone have resulted in billions of compromised records. In 2015, PricewaterhouseCoopers reported a 66% year-over-year increase since 2009 in the compound annual growth rate of detected security incidents.¹ As organizations upgrade software to confront the security risk, cybercriminals devise techniques to evade it. Gartner, a technology research firm, reports that worldwide security software sales reached US\$21.4 billion in 2014, an increase of 5.3% over the previous year.²

While all types of IT security risks continue to increase, your business doesn't have to be vulnerable. You can withstand unexpected security events and avoid risks to your reputation or to customer channels when you prepare in advance for the unknown. Perhaps you've tried to create a program that connects IT risk management to business strategy. Or you want to

SOLUTION PROFILE

remediate recent audit findings by removing your organization's information silos. Maybe you don't know where to begin with an information security program. Whatever your level of security maturity, our information security experts can help you take the next step.

Hitachi Data Systems understands the issues and concerns organizations face when trying to protect critical information. We focus on understanding your business and speaking to you in business terms about your specific risks and priorities.

Hitachi Data Systems Is Your Embedded Security Partner

Many security firms present a laundry list of confusing and overlapping services. It can be difficult to cut through the jargon and determine what you need to support your business. Our security consulting services are divided logically into groups that support an integrated framework of governance, risk management and compliance. To tailor our service offering for your organization, we rely on innovative research and development (R&D) initiatives. We also partner with select security technology providers from around the world.

Our security consulting services have helped organizations in more than 40 countries:

- Identify network vulnerabilities.
- Secure critical data.
- Build and implement comprehensive security programs.
- Avoid onerous fines from failure to meet stringent compliance requirements.

Customers choose us for our human approach, which involves tackling security issues as a long-term, trusted advisor. We discourage quick-fix technology solutions that may not address your business concerns. We believe the human element of security services remains your best defense against cybercrime and data theft.

Services Offerings

Our security service capabilities reflect an integrated framework of governance, risk and compliance functions (see Figure 1).

Specific services in each of these categories include:

Governance	Risk	Compliance
Security Program Review and Design	Risk Assessment Control Assessment	Payment Card Industry (PCI)
IT Security Governance Consulting	Technical Security Testing (TST) Vulnerability Assessment Application Assessment Penetration Testing	

Figure 1. Security Services from Hitachi Data Systems fall into three domains: governance, risk and compliance.

Governance

- Security Program Review and Design.
- IT Security Governance Consulting.

Governance-related consulting and professional services directly support the business leadership of an organization in all things that concern security. This can include:

- Creation from the ground up of a holistic, enterprise-wide security policy.
- Secure development of an organization's infrastructure.
- Formal business and privacy impact assessments to identify the sensitivity and criticality of information assets.

Risk

- Risk Assessment.
- Control Assessment.

These professional services support an organization's corporate risk management process. They include:

- Risk evaluations.
- Policy reviews.
- Architecture assessments.
- Gap reviews against such information security frameworks as International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST).

Compliance

- Payment Card Industry (PCI) Compliance.

Compliance services support your organization's efforts to comply with various regulatory and compliance frameworks. Our current service offering focuses on payment card industry (PCI) compliance activities.

We perform:

- Industry-leading penetration testing.
- Vulnerability assessments.
- Social engineering.
- Web application assessments.

Technical Security Testing

- Vulnerability Assessment.
- Application Assessment.
- Penetration Testing.

Why Rely on Hitachi Data Systems Global Services for Your IT Security?

To help you ensure a safe and secure IT environment that avoids risk and related vulnerabilities, Hitachi Data Systems offers the following service capabilities:

Insightful
Analyst
Report

DOWNLOAD

Security Program Review and Design

What could be more valuable than the confidence that your organization's security program is rock solid? Our security program review and design service combines best practices with leading information security frameworks to develop an enterprise information security program tailored for your organization.

We begin by gaining a detailed understanding of your organization from a business perspective. We learn how your organization operates in its current environment, what business strategies your information technology supports, and your organization's overall risk appetite. We use international control frameworks such as ISO and NIST to assess your current level

of control maturity. We work with you to identify the gaps in your existing controls, then use the control assessment to determine the risks your organization faces.

We also design an “information security bookshelf.” The bookshelf provides a visual representation of the information security controls your organization should have in place to protect the information assets you and our security consultants have identified. We tailor the bookshelf for your organization and base it on internationally recognized standards. Your organization gains a road map for driving the maturity of information security controls. Targeted members of your internal staff also receive the training and advice they need to manage the security program into the future.

Control Assessment

All organizations possess information that is critical or sensitive, ranging from personal, financial and product data to customer, brand and intellectual property. Any gaps in your information security program could reduce the level of protection for these information assets and expose your organization to loss. With a control assessment, we drive your maturing internal security controls into alignment with industry best practices.

If your organization must comply with regulatory requirements, a control assessment will help you prepare for an audit by identifying security gaps. You should consider a control assessment to find out if your environment aligns to your policies or to ask questions about your security program’s effectiveness. Control assessments are also valuable if you have had major changes in your environment or need to merge newly acquired organizations.

Our consultants tailor security architectures, frameworks, methodologies and models to meet your industry needs and compliance requirements. We can perform assessments and reviews for a variety of organizations, from complex enterprises to small and medium businesses. Our services are valuable to industries with multiple regulatory requirements, such as financial services, government, communications, healthcare, energy, retail, and oil and gas.

Risk Assessment

Effective risk management hinges upon a thorough understanding of your organization’s security posture. We can help you gain that understanding.

With a risk assessment, you receive an analysis of risks present in your organizational and technical environment. Our experts are knowledgeable about many security and IT control frameworks, including the Harmonized Threat and Risk Assessment (TRA) methodology, IT Infrastructure Library (ITIL), NIST and the ISO 27000 series of information security management best practices.

In our approach to risk assessment, we:

- **Prepare and plan.** We define the aim, scope and boundaries of your system, define a concept of operation and document a system description.
- **Identify assets and assess sensitivity.** We assess and identify assets according to confidentiality, integrity and availability attributes.
- **Conduct threat analysis.** We identify threat agents and develop scenarios based on the likelihood of attack and the capabilities and motivations of attackers.
- **Conduct vulnerability analysis.** We determine the types of attacks to which system assets are vulnerable and characterize the level of effort (resources and capability) required by an agent to mount an attack.
- **Determine residual risks.** We examine the consequence of threat scenarios and the likelihood of their occurrence. Further, we determine the risk associated with the operation of your IT system.
- **Prioritized remediation plan.** We prioritize all identified risks and provide a final assessment to serve as the basis of an effective, overall risk mitigation strategy.

PCI Compliance Services

Navigating confusing PCI requirements requires considerable effort. We can relieve you of that burden, so you can focus on your business.

To ensure credit card payment security, the Payment Card Industry Security Standard Council (PCI SSC) created the Payment Card Industry Data Security Standard

(PCI DSS). All organizations that handle cardholder information must comply with PCI DSS requirements for safeguarding credit card transactions and personal and financial consumer data.

As a Qualified Security Assessor (QSA), Hitachi Data Systems can help you address all PCI DSS requirements while reducing the complexity and costs associated with compliance. We help you conduct analysis, deploy technology based on the assessment of your requirements, and implement policies and procedures to achieve the highest levels of compliance. To simplify the implementation of necessary policies and procedures, and ensure cardholder data is not being compromised, we can provide:

- Security event log management and monitoring.
- Intrusion detection and prevention system.
- Internal vulnerability scanning.
- External vulnerability scanning.
- File integrity monitoring.

We offer services to:

- Help you complete a PCI Report on Compliance.
- Lead you through a PCI Self-Assessment Questionnaire.
- Conduct advisory services, such as PCI readiness reviews. This works well if your business is required to adhere to PCI DSS, but does not need help with a PCI Report on Compliance or Self-Assessment Questionnaire.

Vulnerability Assessment

Get to the root of your security problems. We can arm you with an exhaustive list of the vulnerabilities on your infrastructure and clear explanations on how to remediate them.

In a vulnerability assessment, we uncover issues in your information systems and offer recommendations to reduce the level of risk facing your IT infrastructure. Security testing of an enterprise information system is not without risk. Our security experts make every effort to ensure that testing is appropriate for the system under investigation. We avoid system disruption and make the most effective use of your organization’s resources and limited testing windows.

Methods used to identify vulnerabilities include:

- Network infrastructure review.
- Vulnerability scanning.
- Scanning validation.
- Network traffic analysis.
- Vulnerability research.

Application Assessment

Web applications that face your customers are your first line of defense against critical intrusion. The security of these applications is often subject to stringent regulatory requirements. With help from our experts, you can rest assured that your applications are safe and compliant.

Our application assessment helps your organization fully understand vulnerabilities in its applications. Our assessments can involve public websites that serve customers, a third-party supplier interface into a corporate customer relationship management (CRM) application, or even standalone applications.

A complete application assessment should go beyond a collection of automated tests and delve deeply into application logic and security controls. We do this by looking for problems in such areas as:

- Privilege escalation to circumvent segregation of duties.
- Extensively customized SQL and XML injection.
- User session handling.
- Inspection of data input fields with fuzzing and manual parameter manipulation.
- Cookie manipulation.
- Business logic bypass actions.
- Other problems named by standards organizations dedicated to Web applications, including the Open Web Application Security Project (OWASP Top 10) and the SANS Institute's Common Weakness Enumeration (CWE/SANS Top 25).

Penetration Testing

Penetration testing is now a regular part of many compliance programs. It also provides a unique insight into organizational risk by concretely demonstrating security failures. Your organization can use penetration testing to determine the likelihood of data loss through software vulnerabilities and hacking activities. With this proactive enterprise-risk-assessment activity, you can strengthen your defenses rather than respond to system damage after incurring damage.

Before performing a penetration test, our experts assess potential targets and related vulnerabilities. Wherever a potentially viable method of exploitation exists, our analysts use it to try to gain unauthorized access to data on your systems. They may also leverage a compromised system to retrieve data from another system.

We use various commercial and open source tools to scan systems for vulnerabilities and perform penetration testing, including:

- Scanning tools:
 - Nmap.
 - Nessus and McAfee vulnerability management.
 - Packet sniffing programs.
 - Enumeration tools built into the Metasploit framework (a tool for developing and executing exploit code against a remote machine).
- Penetration test tools:
 - Network attack tools.
 - Password cracking tools.
 - System exploitation frameworks (Canvas and Metasploit open source tools).
 - Purpose-built programs designed for specific vulnerabilities.

IT Security Governance Consulting

Many organizations need ad hoc security advice that doesn't neatly fit into one of the above service capabilities. To accommodate this need, we offer on-demand access to our world-class security consultants, who are available on a retainer basis to help your organization with security governance and strategy.

This service makes our full suite of security services available to your organization. It is useful for organizations that do not have a chief information security officer (CISO) or have a CISO who is overextended. Many of our consultants have held high-level security positions and are well qualified to deliver CISO-level strategic advice on your information security framework, overall security posture and long-term information security needs.

This ongoing service, designed to augment your existing information security program, provides services as you need them. These services may include executive-level information security workshops on specific security topics and best practices as well as employee-level education and awareness programs.

For More Information

Learn more about how services from Hitachi Data Systems can help you secure your IT environment with minimum risk. Our services can help you quickly realize the benefits of new technology or free you to accelerate your journey to the cloud.

Visit us at: www.hds.com/services.

¹ The Global State of Information Security® Survey 2015 – Managing cyber risks in an interconnected world. PricewaterhouseCoopers, 2015. change to: http://www.pwchk.com/home/eng/rcs_info_security_2015.html

² Gartner Says Worldwide Security Software Market Grew 5.3 Percent in 2014. Press Release from Gartner Newsroom, May 27, 2015. <http://www.gartner.com/newsroom/id/3062017>

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, CA 95050-2639 USA
www.HDS.com community.HDS.com

Regional Contact Information

Americas: +1 866 374 5822 or info@hds.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hds.com
Asia Pacific: +852 3189 7900 or hds.marketing.apac@hds.com

