



# Managed Services Compliance Program **2008**



## Managed Compliance Services Program

*Meeting the Recurring Regulatory & Standard Requirements of ISO 27002 (17799), PCI DSS, HIPAA, Sarbanes-Oxley and Others*

Does your organization need to comply with regulations and standards such as ISO 27002, PCI DSS, HIPAA, Sarbanes-Oxley and others? Are your internal resources stretched to capacity and you lack the necessary expertise to identify all compliance gaps and security vulnerabilities? More than ever before, businesses today need to comply with regulatory requirements to protect sensitive information about their customers, who may be consumers or patients. The penalties associated with not meeting compliance requirements are not insignificant. Further, organizations have to expend precious internal resources to gain compliance expertise and then manage regulatory requirements for privacy and information on a recurring basis. This can be challenging to most organizations. ecfirst can help with its Managed Compliance Services Program – the first program of its type in the industry, worldwide.

With over 900 clients since 1999 and recognized as an Inc. 500 firm – America's fastest growing Top 500 privately held business in 2004, ecfirst has enabled hundreds of organizations all across the United States and abroad, achieve and maintain compliance with regulations and standards that impact their business. ecfirst delivers compliance capabilities through its Managed Compliance Services Program – the first of its type in the industry, worldwide.

Legislation mandates require organizations to maintain compliance with reasonable and appropriate safeguards in several specific areas. Compliance requirements result in critical activities that must be conducted on a regular schedule, typically once a year.

### **On a regular schedule, organizations must:**

- Assess compliance with the requirements of confidentiality and privacy related regulations
- Assign responsibility to the security officer who is responsible for coordinating compliance and security initiatives
- Conduct a comprehensive and thorough risk analysis including vulnerability assessment (penetration testing)
- Complete a Business Impact Analysis (BIA) for contingency planning and disaster recovery
- Develop and update security policies and procedures
- Train all members of the workforce
- Audit and evaluate the information infrastructure

## Executive Summary of Managed Service

The ecfirst **Managed Compliance Services Program** is tailored to meet your compliance requirements. Key features of the ecfirst Managed Compliance Services Program are:

- Bundled outsourced solution for a **fixed monthly fee**
- Periodic performance of vulnerability assessments, security risk analysis, BIA and contingency planning
- Training, certification and periodic audit and evaluation to keep your organization fully compliant at all times
- Keeping you compliant with the regulations, to help you focus on the business of delivering exceptional services and capabilities to your clients

Benefits of outsourcing compliance and security include:

- Minimizing productivity losses from unexpected downtime
- Enabling staff to better focus on business-critical tasks and complying with key regulations
- Depth in resource capabilities with trusted knowledge of client infrastructure
- Smooth out volatility in resource demands and costs associated with managing information technology

Figure 1 summarizes key areas addressed by the ecfirst Managed Compliance Services Program.



Figure 1: ecfirst's Managed Compliance Services Program.

ecfirst's Managed Compliance Services Program is designed to address critical regulatory requirements. This program allows customers to outsource their regulatory activities which will lower costs and save time. The Global Managed Compliance Center is a highly flexible and scalable service.

## Specific Service Offerings

Figure 2 summarizes information about ecfirst's Managed Compliance Service Offerings:

Sample Regulatory Requirement	Regulatory Description	Service Offerings
Privacy/Confidentiality Review	Establish capabilities for accessing sensitive customer or client information that the organization comes into contact with.	<ul style="list-style-type: none"> <li>Review access controls for access to sensitive information</li> <li>Review privacy policies and procedures</li> <li>Identify privacy compliance gaps</li> </ul>
Assigned Security Responsibility	Organizations must identify the security official who is responsible for the development and implementation of the regulation's required policies and procedures.	<ul style="list-style-type: none"> <li>Additional capability as an Interim Security Officer to oversee risk and compliance</li> <li>Inclusion of security responsibility as part of the job roles and responsibilities</li> <li>Inclusion of security requirements in third party contracts / agreements</li> </ul>
Risk Analysis	Conduct an accurate and thorough assessment of the potential risks to and vulnerabilities of the confidentiality, integrity and availability of the organization's sensitive information.	<ul style="list-style-type: none"> <li>Assess IT processes</li> <li>Classify data/assets (CIA)</li> <li>Assess threat likelihood on assets/services</li> <li>Impact Analysis on information assets</li> <li>Evaluate the adequacy in current levels of controls and safeguards</li> <li>Risk mapping and classification</li> <li>Analyze controls gaps</li> <li>Identify remediation priorities</li> <li>Prepare standardized reports</li> </ul>
Contingency Plan	Organizations must establish policies and procedures for responding to an emergency.	<ul style="list-style-type: none"> <li>Assess Business Processes</li> <li>Conduct Business Impact Analysis (BIA)</li> <li>Analyze existing recovery plan and contingency measures</li> <li>Develop recovery strategies</li> <li>Develop contingency plan documents</li> </ul>
Policies, Procedures and Documentation	Organizations must implement reasonable and	<ul style="list-style-type: none"> <li>Review policy and procedure</li> </ul>

	appropriate policies and procedures to comply with regulatory requirements.	<p>implementation plan</p> <ul style="list-style-type: none"> <li>• Review of the existing information security policies and map to regulatory requirements</li> <li>• Develop additional policies to address policy gaps</li> <li>• Help process owner in implementing the procedures to comply with regulatory requirements</li> <li>• Develop a document standard for policies and procedures</li> </ul>
Security Awareness and Training	Organizations must implement a security awareness and training program for all members of the workforce.	<ul style="list-style-type: none"> <li>• Periodic training and awareness programs on security policies for employees and contractors</li> <li>• Identify role based training for operations and support staff to address compliance requirements</li> <li>• Develop training content to address regulatory requirements</li> </ul>
Evaluation	Organizations must perform periodic evaluations to determine the extent to which the security policies and procedures meet regulatory requirements.	<ul style="list-style-type: none"> <li>• Periodic review of information security policies and procedures</li> <li>• Review changes to regulatory requirements and make necessary changes to policies</li> <li>• Update standards, baselines, procedures to comply with policies</li> <li>• Develop dashboard reporting to clearly establish state of compliance</li> <li>• Assess remediation actions recommended in risk analysis and actual actions taken by the organization to mitigate risk</li> </ul>

Figure 2: Managed Compliance Service Offering.

## Additional Value Added Services

Our service offerings are aligned with regulations to ensure complete compliance for your organization. Additional value added services offered by ecfirst include:

- Advisories on Security vulnerabilities and fixes
  - Security alerts and mailers
  - Regular advisories on security vulnerabilities
- Security Monitoring and Management Services
  - Centralized security monitoring & event correlation
  - Perimeter security monitoring
- Patch / Release Management
  - Centralized management for patch deployment activity
  - Automated process for patch deployment
  - Patch testing

- Patch status reporting
- Security Incident Management
  - Develop incident management framework
  - Incident detection and classification
  - Diagnosis and investigation
  - Incident Reporting
- Log monitoring and event correlation
  - Log analysis and event correlation
  - Trend analysis, pattern recognition
  - Storage and retention
- Compliance Dashboards, trends and statistics
  - Compliance reports and dashboard
  - Statistical analysis

## **Program Benefits**

ecfirst provides world class infrastructure services through the acclaimed Global Infrastructure Command Center and security services through the Global Security Operations Center. Our Managed Compliance Services Program is designed to assist healthcare organizations and business associates manage compliance requirements, security and core components of the Infrastructure. ecfirst's Managed Compliance Services Program is designed to address critical regulatory requirements. Key benefits of the ecfirst managed services program include:

- Clearly defined deliverables to achieve compliance
- Expert advisor assigned – serves as interim security advisor
- Risk analysis and business impact analysis conducted on a regular schedule
- Policies maintained on a continual basis
- Easily tailored to your organizational requirements
- Very scalable program – can monitor and audit as required
- Skilled resource pool with expert domain knowledge
  - Enables your staff to focus on your business and us on compliance
- Fixed monthly fee

The ecfirst Managed Compliance Services Program provides a 360<sup>0</sup> end to end compliance service spectrum that can be tailored to meet your specific requirements.

## About ecfirst

ecfirst is a leader with rich hands-on experience delivering world-class services in the areas of:

- Security regulatory compliance solutions (HIPAA, FISMA, ISO, PCI DSS, Sarbanes-Oxley)
- Compliance training and certification
- Professional staffing, including project management



### Regulatory Compliance Practice

The ecfirst Regulatory Compliance Practice delivers deep expertise with its full suite of services that include contingency planning/Business Impact Analysis (BIA), secure single sign-on, vulnerability assessment, as well as managed security and IT infrastructure solutions.

### Compliance and Training certification

ecfirst, home of the HIPAA Academy, offers the gold standard in compliance training and is endorsed by the American Hospital Association (AHA). The HIPAA CHA™, CHP and CHSS™ certifications are the only certifications recognized in the Industry. The ecfirst Certified Security Compliance Specialist™ (CSCS™) Program is the first and only information security program that addresses all major compliance regulations from a security perspective.

### Credentialed Professional Staffing Practice

The ecfirst Professional Staffing Practice excels in meeting your short and long term requirements for contract professionals in the areas of Web development, IT and project management. This practice is distinguished with credentialed staff (PMP, CBCP, CISSP, CSCS™ or CHSS™) that includes deep industry knowledge in the healthcare, financial and government markets.

ecfirst assists all types of organizations with their compliance initiatives for a secure information infrastructure that is compliant with regulation requirements. ecfirst can help you with your compliance challenges and priorities. ecfirst solutions help your organization implement the security safeguards required as a result of the legislation requirements.

ecfirst, an Inc. 500 business, serves a Who's Who client list that includes Wells Fargo, U.S. Veterans Agency, numerous hospitals, state and county governments (State of Oregon, Iowa, Illinois), and hundreds of other organizations.

We understand that if, and only if, we deliver exceptional value to your organization in every instance of our engagement, will we be able to have you as a customer for life. All our work is executed with deep knowledge of your industry and compliance requirements by quality staff with certifications that substantiate their expertise. We are always striving to earn your trust.

For more information, please visit <http://www.ecfirst>.

## ***Endorsed by the American Hospital Association (AHA)***

ecfirst is proud of being exclusively selected by the American Hospital Association (AHA) as its strategic partner for delivering HIPAA Training and Certification.



The American Hospital Association (AHA) has endorsed solutions from ecfirst, Inc.'s (ecfirst) HIPAA Academy as a resource for training and certification to help hospitals comply with the newly enacted Health Insurance Portability and Accountability Act (HIPAA) security regulations.

The HIPAA security regulations require certain healthcare payers, providers and healthcare clearinghouses to establish procedures and mechanisms to protect the confidentiality, integrity and availability of electronic protected health information (EPHI), and to ensure the restoration of lost data. Acquisition of expert knowledge on the regulations and understanding applicable solutions options for complete compliance can be a challenge to resources at hospitals and other healthcare providers, yet HIPAA is a federal requirement and not an option for all covered entities.

While compliance with the security rule cannot be achieved through new information systems alone, the AHA is pleased to bring additional HIPAA resources to the forefront for its members. Achieving compliance will require attention from a hospital's compliance, legal, and information technology departments.

After an intense evaluation, the AHA selected ecfirst, home of the HIPAA Academy, because of its subject-matter expertise in healthcare, the technical excellence and depth of its HIPAA training and certification programs, and its strong track record in serving the healthcare marketplace.

## ***U.S. Department of Veterans Affairs - Testimonial***



WASHINGTON, April 27, 2006 – The U. S. Department of Veteran’s Affairs faced a daunting task – choosing an organization to train the nation’s VA Hospitals’ Privacy and Security Compliance officials on the Health Insurance Portability and Accountability Act (HIPAA). Since each official was responsible for compliance with the federal regulation protecting patient data for their respective hospital, a comprehensive training program was required. HIPAA Academy, a division of ecfirst, was chosen based on their reputation in the healthcare industry for high-quality and comprehensive HIPAA training solutions.

“HIPAA Academy is one of the finest educational organizations with whom I have had the pleasure to work. The staff are extremely knowledgeable and experienced both in private sector and government sector security legislation” stated Lydia Duckworth, HIPAA Security Project Manager for the VA.

Uday ‘Ali’ Pabrai, CEO of HIPAA Academy, was involved n the project from the beginning and delivered the security training. “During our work together, Ali Pabrai was able to impart best practices for developing disaster recovery plans, the technical specifications for public key infrastructure and other encryption based solutions, wireless security requirements and the general state of HIPAA Security compliance.”

“I welcome the opportunity to work with HIPAA Academy again in the future and would recommend this organization to anyone looking to develop security or privacy training tailored to their particular environment whether you are a healthcare organization or a business associate of a health care organization”, said Duckworth.

### **About the U.S. Department of Veterans Affairs**

The Department of Veterans Affairs (VA) is responsible for providing federal benefits to veterans and their families. Headed by the Secretary of Veterans Affairs, VA is the second largest of the 15 Cabinet departments and operates nationwide programs for health care, financial assistance and burial benefits. VA’s health care system now includes 154 medical centers, with at least one in each state, Puerto Rico and the District of Columbia. VA operates more than 1,300 sites of care, including 875 ambulatory care and community-based outpatient clinics, 136 nursing homes, 43 residential rehabilitation treatment programs, 206 Veterans Centers and 88 comprehensive home-care programs. VA health care facilities provide a broad spectrum of medical, surgical and rehabilitative care.