bizSHIELD tm

ecfirst | Perfecting the Art of *Active* Cyber Defense

ecfirst Services

BBB ACCREDITED BUSINESS

Table of Contents

Hospitals, health systems, physician practices, payers such as insurance organizations, as well as business associates must conduct a comprehensive risk analysis exercise to meet HIPAA mandates, including HITECH Meaningful Use requirements. Security standards such as ISO 27000 and NIST guidelines require a thorough risk assessment.

Have you completed a risk analysis exercise recently?

Risk Analysis Solutions

bizSHIELD tm

Risk Analysis: Critical for a Information Security Baseline

A key requirement of the HIPAA and HITECH regulations is that covered entities and business associates *must conduct a comprehensive and thorough assessment of the potentials risks and vulnerabilities to the confidentiality, integrity, and availability (CIA) of all electronic Protected Health Information (EPHI)*. These HIPAA and HITECH mandates require that organizations must complete a comprehensive and thorough vulnerability assessment on a regular schedule.

OCR Guidance on HIPAA Risk Analysis

The guidance published by the Office of Civil Rights states that, “Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational…” Further, OCR states that “All EPHI created, received, maintained or transmitted by an organization is subject to the Security Rule.

The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of EPHI. Risk analysis is the first step in that process."

*ecfirst's biz*SHIELD^tm^ *program satisfies this HIPAA requirement.*

HITECH Meaningful Use Requirements Include Risk Analysis

Demonstrating Meaningful Use of an Electronic Health Record (EHR) requirement tells organizations that they must, "Implement systems to protect the privacy and security of patient data." Organizations seeking to demonstrate Meaningful Use must, "Conduct or review a security risk analysis and implement security updates as necessary and correct identified security deficiencies."

*ecfirst's biz*SHIELD^tm^ *program satisfies this HITECH requirement.*

*biz*SHIELD^tm^ – An ecfirst Risk Analysis Service

ecfirst developed the *biz*SHIELD^tm^ program to assist Covered Entities, Business Associates, and vendors of Electronic Health Records (EHRs) and Personal Health Records (PHRs) in meeting the requirements of the HIPAA Privacy and Security Rule, The HITECH Act, and all subsequent guidance documentation and settlement agreements.

As a part of the *biz*SHIELD^tm^ program, ecfirst will list every requirement of the HIPAA Security Rule including every Safeguard, Standard, and Implementation Specification in a risk analysis format that identifies an organization's state of compliance with the requirement, recommended remediation activity, and associated risk priority. All remediation activities will be listed according to recommended implementation time bands in the *biz*SHIELD^tm^ Corrective Action Plan (CAP) table. The *biz*SHIELD^tm^ report is an actionable, documented risk analysis that provides both in depth and executive summary level findings appropriate to all audiences from administrators to the Board of Directors.

Privacy Gap Assessment Service

*biz*SHIELD^tm^ helps an organization to understand, improve, or verify their compliance with the HIPAA Privacy Rule. *biz*SHIELD^tm^ provides both summary and detailed compliance information as well as all necessary remediation activities pertinent to the organization's business model. *biz*SHIELD^tm^ will enable an organization to quickly determine the state of compliance, needed remediation, and will list actionable steps to achieve compliance.

HITECH Data Breach Service

Under the HITECH Data Breach Rule, organizations are required to take steps to prevent, identify, report, and remediate data breaches of unsecured information. The ecfirst Data Breach solution will document the ability of the organization to detect a breach, review the incident management policy and procedures, and make recommendations. In addition, organizations will receive a HITECH Data Breach policy and several Data Breach procedures to ensure compliance, should a breach happen.

Return to Table of Contents

Hospitals, health systems, physician practices, payers such as insurance organizations, as well as business associates must conduct a comprehensive risk analysis exercise to meet HIPAA mandates, including HITECH Meaningful Use requirements. Security standards such as ISO 27000 and NIST guidelines require a thorough risk assessment.

Have you completed a technical vulnerability assessment exercise recently?

Technical Vulnerability Assessment

*biz*SHIELD tm

HIPAA & HITECH Require Technical Vulnerability Assessment

A key requirement of the HIPAA and HITECH regulations is that covered entities and business associates *must conduct a comprehensive and thorough assessment of the potentials risks and vulnerabilities to the confidentiality, integrity, and availability (CIA) of all electronic Protected Health Information (EPHI)*. These HIPAA and HITECH mandates require that organizations must complete a comprehensive and thorough vulnerability assessment on a regular schedule.

*biz*SHIELD^tm^ – An ecfirst Technical Vulnerability Assessment Service

ecfirst developed the *biz*SHIELD^tm^ program to assist Covered Entities, Business Associates, and vendors of Electronic Health Records (EHRs) and Personal Health

Records (PHRs) in meeting the requirements of the HIPAA Privacy and Security Rule, The HITECH Act, and all subsequent guidance documentation and settlement agreements.

As a part of the *biz*SHIELD^{tm} program, ecfirst will list every requirement of the HIPAA Security Rule including every Safeguard, Standard, and Implementation Specification in a risk analysis format that identifies an organization's state of compliance with the requirement, recommended remediation activity, and associated risk priority. All remediation activities will be listed according to recommended implementation time bands in the *biz*SHIELD^{tm} Corrective Action Plan (CAP) table. The *biz*SHIELD^{tm} report is an actionable, documented risk analysis that provides both in depth and executive summary level findings appropriate to all audiences from administrators to the Board of Directors.

Technical Vulnerability Assessment Service

The Office of Civil Rights (OCR) wants to ensure that organizations have identified all of the risks and vulnerabilities to the EPHI that they collect, store, process, or transmit. The ecfirst *biz*SHIELD^{tm} risk analysis program includes a technical vulnerability assessment to address HIPAA and HITECH mandates with the objective of establishing and prioritizing compliance and security gaps. The ecfirst *biz*SHIELD^{tm} Technical Vulnerability Assessment Service supports several distinct components, including:

- External Assessment
- Internal Assessment
- Firewall Assessment
- Wireless Assessment
- Social Engineering

When was the last time your organization conducted a risk analysis activity that included a technical vulnerability assessment?

External Network Vulnerability Assessment

ecfirst will identify, analyze, and document vulnerabilities within an organization's Internet-facing infrastructure and attached systems. ecfirst follows a pragmatic approach when conducting a vulnerability assessment of external systems.

Internal Network Vulnerability Assessment

ecfirst's internal network vulnerability assessment will verify that the security controls implemented on an organization's hosts provide an adequate level of protection against network attacks. The ecfirst security team will scan and validate the security of the network and perform a comprehensive assessment against selected hosts. ecfirst can include many valuable components in its reporting including:

- Active Directory assessment
- Open File Shares scan and report
- SNMP scan
- Promiscuous NICs scan and report
- Database Security Analysis including MS SQL or Oracle

Firewall Assessment

ecfirst will review the organization’s Internet-facing firewall to identify the current security posture in three critical areas:

- Rulebase configuration
- Current IOS (or other operating system) and patch revision release level
- Vulnerability assessment of configuration file

Rulebase configuration is critical to the integrity and operating security of a firewall. The rulebase should be tied to business requirements. Every rule that is configured on a firewall is essentially a permissible security hole into the company’s network infrastructure. Each of these rules should have a well-defined business need for existing. However, many corporations open rules for testing and never close them when the test has completed. Additionally, many rules are opened up because of then-current business needs, but never closed or repaired once that need, or the corresponding business contract, has ended. This results in legacy access and a vulnerability providing a pathway into the internal network.

Wireless Assessment

Wireless networks are particularly vulnerable to attacks because it is extremely difficult to prevent physical access to them. Wireless networks are subject to both passive and active attacks. A passive attack is one in which an attacker just captures signals flowing from authorized devices, such as a corporate laptop to an authorized Access Point (AP). An active attack is one in which an attacker send signals to the authorized AP in order to solicit specific responses and intrude upon the corporate network, typically, in a very short timeframe.

During the wireless assessment, ecfirst addresses the following areas:

- Discover the Wireless Access Points and wireless systems.
- Investigate rogue devices installed without IT department consent.
- Assess Wi-Fi RF coverage from adjacent buildings and public locations.

- Determine the existing Wi-Fi security infrastructure.
- Attempt to compromise the wireless security.
- Determine encryption type and compromise the security.

Social Engineering Assessment

Organizations with excellent security programs often spend large amounts of money on capital purchases to implement technical security controls. However, employees or contractors of the entity often prove to be the weak link in the security chain. Employee and contractor education is a key component to any information security program. Authorized members of the workforce have both authenticated access to information systems as well as physical access to facilities and secured areas.

During the social engineering assessment, ecfirst will attempt to gain unauthorized or inappropriate access to facilities, secured areas, documents, credentials, or confidential data. ecfirst security personnel will attempt to bypass security controls that are in-place in order to gain access to various assets. ecfirst will attempt to bypass electronic, personnel, and procedural controls during this assessment. ecfirst will document and present a very detailed record of successes, failures, controls bypassed, access achieved and information obtained during the assessment.

Return to Table of Contents

BIA & IT Disaster Recovery Plan

Prepared for a Disaster?

bizSHIELD tm

Contingency planning, also referred to as Business Continuity Planning (BCP), is a coordinated strategy that involves plans, procedures and technical measures to enable the recovery of systems, operations, and data after a disruption. A Business Impact Analysis (BIA) is the foundation for building Contingency Plans.

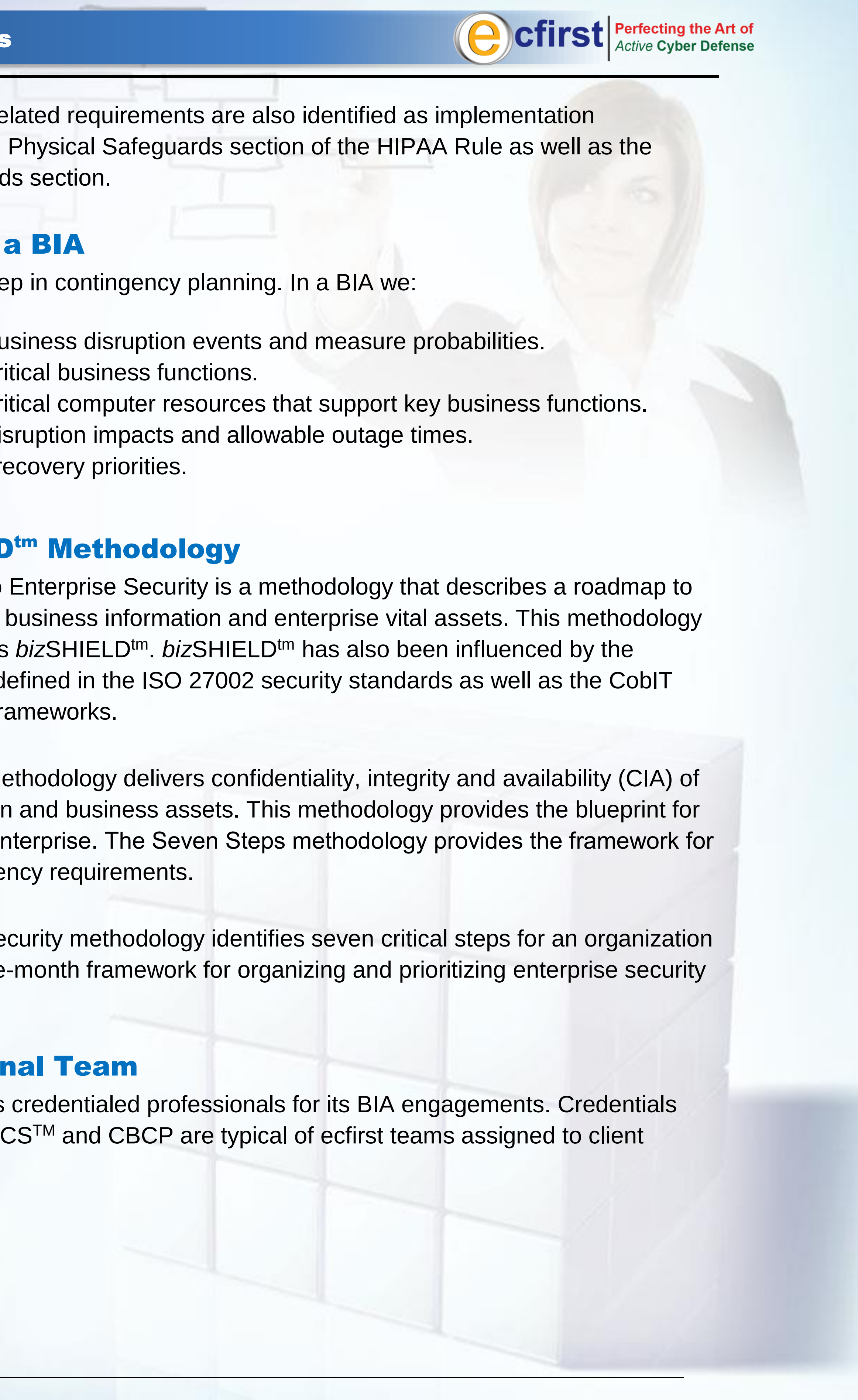
Once the BIA is completed, Contingency Plans can be developed using the information identified in the BIA. Typically, two types of Contingency Plans will need to be developed: Emergency Mode Plans for business unit recovery and Disaster Recovery Plans (DRP) for Information Technology (IT) systems and infrastructures.

Compliance Mandate

Contingency Plan is a HIPAA Security Standard. It is also a Clause in the ISO 27000 Security Standard. The objective of the Contingency Plan Standard is to establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI. As shown in bold in the table below, the Contingency Plan standard is defined within the Administrative Safeguards section of the HIPAA Security Rule.

Standards	Implementation Specifications	R = Required
		A = Addressable

Contingency Plan	Data Backup Plan Disaster Recovery Plan Emergency Mode Operation Plan Testing and Revision Procedure Applications and Data Criticality Analysis	R R R A A



Contingency Plan-related requirements are also identified as implementation specifications in the Physical Safeguards section of the HIPAA Rule as well as the Technical Safeguards section.

It Starts with a BIA

A BIA is a critical step in contingency planning. In a BIA we:

1. Identify business disruption events and measure probabilities.
2. Identify critical business functions.
3. Identify critical computer resources that support key business functions.
4. Identify disruption impacts and allowable outage times.
5. Develop recovery priorities.

Our *biz*SHIELD^tm^ Methodology

The Seven Steps to Enterprise Security is a methodology that describes a roadmap to safeguard sensitive business information and enterprise vital assets. This methodology is also referred to as *biz*SHIELD^{tm}. *biz*SHIELD^{tm} has also been influenced by the clauses (domains) defined in the ISO 27002 security standards as well as the CobIT and NIST security frameworks.

The *biz*SHIELD^{tm} methodology delivers confidentiality, integrity and availability (CIA) of your vital information and business assets. This methodology provides the blueprint for defending today's enterprise. The Seven Steps methodology provides the framework for addressing contingency requirements.

The *biz*SHIELD^{tm} security methodology identifies seven critical steps for an organization to follow as a twelve-month framework for organizing and prioritizing enterprise security initiatives.

Our Professional Team

ecfirst only engages credentialed professionals for its BIA engagements. Credentials such as CISSP, CSCS^{TM} and CBCP are typical of ecfirst teams assigned to client engagements.

Your Commitment to Us

1. Interviews with key members of IT staff, key individuals in departments and management.
2. Copies of IT system and network documentation including downtime procedures and inventory of vital assets such as servers and applications.

Our Deliverables to You

A *biz*SHIELD^{tm} Business Impact Analysis (BIA) document will be created based on our review and analysis of information collected from your organization. This *biz*SHIELD^{tm} Business Impact Analysis (BIA) Report will include information in the following areas:

- **Business Risk Assessment**
  - Key business processes identification
  - Time-bands for business service interruption management
  - Financial and operational impact
- **Key Sensitive Systems and Applications Summary**
- **Emergency Incident Assessment**
  - BIA process control summary for emergency incident assessment
  - Serious information security incidents
  - Environmental disasters
  - Organized and/or deliberate disruption
  - Loss of utilities and services
  - Equipment or system failure
  - Other emergency situations

Fixed Fee with a Monthly Payment Schedule: Call for details and a customized proposal exclusively for your organization. *On-Demand Compliance Solutions from ecfirst provides your organization with access to specialized compliance and security skills with no short term or long term commitments. Get Started Today!*

Return to Table of Contents

ISO 27000 Solutions

Applying ISO 27000 to Comply with Federal & State Regulation Mandates

*biz*SHIELD^tm

Organizations are increasingly considering applying the family of ISO 27000 international security standards to comply with various U.S. federal and state regulations such as HIPAA, HITECH, as well as standards such as the PCI DSS. The ISO 27000 is a global standard that provides a comprehensive framework that organizations can adopt to address compliance requirements and establish a resilient information infrastructure.

ecfirst Brings Deep Experience & Expertise with ISO 27000

ecfirst's fast-paced, one-day private training workshop on ISO 27000, its policy templates, quick reference cards, and deep consulting expertise embodied in its signature methodology, *biz*SHIELD^{tm}, are enabling organizations to easily adopt the ISO standard. The ecfirst *biz*SHIELD^{tm} is a signature methodology is specifically focused on the ISO 27000 standard and includes the following core components:

- A fast paced, instructor-led, one-day Getting Started with the ISO 27000 (ISO 27001 and ISO 27002) training delivered at your site.
- A two-day in-depth certification program, Certified Security Compliance Specialist^{TM} (CSCS^{TM}) that addresses ISO 27000, PCI DSS, HIPAA, HITECH, FISMA and a lot more.
- A one-day workshop on Getting Started with ISO 27799 that tailors the ISO 27002 Standard for the healthcare industry; the workshop is an industry first from ecfirst.
- ISO 27002 Security Policy Templates that can easily be tailored to enable your organization to establish a comprehensive library of policies.
- The industry's first ISO 27002/HIPAA Security Rule Mapping Framework document.
- Managed Compliance Services Program (MCSP) for ISO 27000 that enables your organization to leverage deep ecfirst ISO expertise and yet pay a fixed monthly fee for a 36-month period and access a range of services at a fixed price.
- ISO 27000 Webcast – Applying the ISO 27000 Standard to Address Federal and State Regulations.

Our Commitment to You

1. Manage the implementation of ISO 27000 in your environment leveraging as best as possible existing information security processes, practices and capabilities
2. Document all information requested and establish time-line for critical next steps
3. Respond with required information and communicate with all involved parties on activities and status
4. Establish framework for complete knowledge transfer to enable your organization to improve processes and capabilities

ISO 27000 Client Consulting Testimonial

“When GHX began discussing our march toward HIPAA compliance, there was a general consensus about where we had to be - in three years, but there was also a notable lack of agreement on how we might get there. After thoughtful consideration (and amazing good fortune) we chose to seek the services of ecfirst as our “implementation partners” to assist our efforts with HIPAA using ISO 27000 as the framework.”

“I’m happy to say, it was the best choice we could have made. Their ISO 27000 experience, comprehensive approach, and practical guidance, have put us solidly on the road to achieving our goal, within our window. For GHX, achieving compliance is huge effort, and having a dependable ally was critical to our success.”

Patt Anderson, *Compliance Manager*
GHX

ISO 27000 & ISO 27799 Training & Certification

ecfirst has several options for ISO 27000 training - from a tailored 60-minute webcast to a two-day CSCS^{TM} certification program. Schedule our one-day training workshop, *“Getting Started with ISO 27000,”* to learn more about the ISO 27001 and ISO 27002 information security standards and understand how these may be applied to address compliance requirements.

1. Examine the ISO 27000 information security framework and its core components.
2. Review the ISO 27001 security standard and understand key terminology, definitions and the overall organization.
3. Step through the clauses defined in the comprehensive ISO 27002 standard.
4. Understand how compliance requirements of State regulations such as those from Massachusetts and California, as well as federal requirements such as HIPAA and HITECH can be addressed with the ISO 27000 framework.
5. Identify critical steps for organizations to get started with the ISO 27000.

Consider the *"Getting Started with ISO 27799"* training workshop. **It is the industry's first training program that brings together the ISO 27000 Standard tailored to the healthcare industry.** This one-day training program can be delivered at your site. ecfirst can customize the content to meet the specific requirements of your organization

Testimonials

"The ISO 27000 Webinar in addressing HITECH, HIPAA & State Regulations was first rate. Looking forward in continuing our involvement with ecfirst in regard to consulting, training and certification. Please send my best to Ali Pabrai, he is a great speaker!"

Juan M. Chavez, *MHA, Risk Management Analyst*
Catholic Healthcare West

"I really liked the detailed overview of ISO 27001/27002, and the heads up on the upcoming ISO 2700X standards. I liked the note about a written comprehensive InfoSec program being needed."

Jim Brady, *Manager, Data Center Services*
Cedars-Sinai Medical Center

"I attended the ISO 27001/2 webcast. It was excellent."

Sishir Reddy, *CEO*
Episource LLC

"The ISO 27000 brief was very helpful as my organization works to implement ISO 27000 for our security framework. I have been CHP and CHSS^{TM} certified by ecfirst for several years and value ecfirst's expertise. I am interested in the CSCS^{TM} certification and will be looking into ecfirst's training program for this certificate."

Judi Hofman, *CAP, CHP, CHSS*
Privacy/Information Security Officer
Cascade Healthcare Community

"I found the program to give me a wonderful framework with the ISO 27000 to enhance our security program under HIPAA and HITECH. The tools will be very helpful in the continued effort to move our program forward."

Lori A Beeby, *Information Systems Director*
Community Hospital – McCook

Return to Table of Contents

PCI DSS Solutions

Readiness Assessment Services

bizSHIELD tm

PCI DSS: An Important Security Standard

The Payment Card Industry (PCI) Data Security Standard (DSS) is *a global information security standard* for protecting cardholder data. The PCI DSS requirements apply to merchants and other organizations that store, process, or transmit cardholder data. PCI DSS is a compilation of best practices for securing data throughout the information lifecycle. The PCI standard identifies several processes and procedures required to protect cardholder data. With unmatched laser beam focus on regulatory compliance and information security.

ecfirst has the services that organizations need to prepare for and deliver on PCI compliance today.

The core goals of PCI DSS include:

1. Remove sensitive authentication data and limit data retention
2. Protect the perimeter, internal, and wireless networks
3. Secure payment card applications
4. Monitor and control access to systems
5. Protect stored cardholder data
6. Finalize remaining compliance efforts, and ensure all controls are appropriately implemented

The ecfirst PCI Readiness Assessment

This assessment enables organizations to understand the current PCI standard compliance posture and includes a Corrective Action Plan (CAP). This plan is a remediation roadmap that the organization should complete prior to undergoing a formal PCI audit.

ecfirst Brings Deep Experience & Expertise with PCI DSS

The ecfirst PCI DSS Readiness Assessment is a methodical examination and review of the state of PCI compliance with the defined control objectives and associated requirements of version 3.0 of the Standard. This ecfirst exercise results in an actionable & comprehensive PCI DSS Readiness Assessment Report that summarizes findings and provides details about areas in which the organization does not comply with version 3.0 of the Standard. A prioritized list of activities and recommended timetable are included, as is an executive presentation of the assessment findings.

The ecfirst PCI Solution addresses requirements in the areas of:

- Discover cardholder assets
- Identify compliance gaps
- Address individual requirements and prevent data breaches
- Ease the compliance process

ecfirst's fast-paced, one-day private training workshop on PCI DSS, its policy templates, quick reference cards, and deep consulting expertise embodied in its signature methodology, *biz*SHIELD^{tm}, are enabling organizations to address PCI DSS requirements. The ecfirst *biz*SHIELD^{tm} is a signature methodology is specifically focused on the PCI DSS standard and includes the following core components:

- A fast paced, instructor-led, one-day Getting Started with the PCI DSS training delivered at your site.
- A two-day in-depth certification program, Certified Security Compliance Specialist^{TM} (CSCS^{TM}) that addresses ISO 27000, PCI DSS, HIPAA, HITECH, FISMA and a lot more.
- Security Policy Templates that can easily be tailored to enable your organization establish a comprehensive library of policies.
- Managed Compliance Services Program (MCSP) for ISO 27000 that enables your organization to leverage deep ecfirst ISO expertise to address PCI DSS mandates; pay a fixed monthly fee for a 36-month period and access a range of services at a fixed price.
- ISO 27000 & PCI DSS Webcast – Applying the ISO 27000 Standard to Address PCI DSS Mandates.

Our Commitment to You

1. Manage the implementation of PCI DSS in your environment leveraging as best as possible existing information security processes, practices and capabilities.
2. Document all information requested and establish time-line for critical next steps.
3. Respond with required information and communicate with all involved parties on activities and status.
4. Establish framework for complete knowledge transfer to enable your organization to improve processes and capabilities.

Key Deliverable

The *biz*SHIELD^{tm} PCI DSS Readiness Assessment Report

- Executive Summary of priority observations and recommendations.
- Gap Analysis, a security assessment sorted by risk and compliance level.
- Detailed breakdown of key findings, concerns, and recommendations for each of the requirements defined in the PCI DSS Standard version 3.0.
- Completion of the appropriate PCI Self Assessment Questionnaire (SAQ) as defined by the PCI Security Standards Council.
- Completion of the PCI DSS v3.0 Prioritized Approach Spreadsheet as defined by the PCI Security Standards Council (based on the prioritized approach to pursue PCI DSS compliance).
- PowerPoint presentation of executive summary (optional).

Return to Table of Contents

On-Demand Compliance Solutions

A Flexible Consulting Service Starting @ 40 Hours Commitment

We at ecfirst refer to this consulting model as, *"You can do it, we can help!"* ecfirst resources may be applied to work along with your IT and compliance personnel to help create and update information security policies, technical procedures, processes, forms, supporting documentation and other required tasks.

You also have the option to consider our Managed Services Compliance Program (MCSP) – a 36-month program based on a fixed fee each month with compliance, security and remediation services delivered on a mutually agreed to schedule over the three year time period.

The ecfirst On-Demand Solution is highly flexible and includes the following characteristics:

- Fixed, flat rate service
- Starting at a minimum 40-hour commitment
- Delivered anywhere in the United States or abroad
- Highly specialized information security skills
- Experienced compliance expertise
- Mix and match skills
- 2-page contract
- Get started with resource commitment immediately

ecfirst can support your compliance remediation or information security activities with specialized resources such as:

- A project manager with expertise in information security; and
- A technical professional with extensive security experience, to enable your organization to address compliance and security project activities.

The scope of work includes the following areas for which ecfirst can provide expert security resources, on-site or off-site, as mutually determined, to address identified compliance gaps or security initiatives such as implementation of controls including firewalls, single sign-on, and others.

The list below represents a **possible example** set of tasks and activities that ecfirst security personnel may be assigned to and assist with. A formal list will be established at the start of the engagement and may be adjusted as mutually determined by both organizations. Additionally, both organizations will mutually determine what activities are required to be completed on-site and what tasks may be executed off-site. Accomplishing some tasks off-site will enable your organization to reduce the expense of the engagement. Time-lines, reporting structure and frequency are to be mutually determined. A sampling of possible tasks and activities include:

- Develop and manage a Project Plan compliance and security priorities and timelines;
- Perform Project Management duties and provide technical implementation assistance to enable your organization in addressing HIPAA Security, HITECH, PCI DSS or ISO 27002 remediation priorities;
- Develop and manage policies to address proactive auditing;
- Develop a program, procedures, and logs to combine and filter audit logs, network activity review, and application security access reviews;
- Develop a program policy to address server security log review;
- Assist in developing Incident Management capabilities, policy, and technical procedures;
- Assist in identifying and investigating potential security violations, and recommend or document appropriate action;
- Establish next steps for implementing SSO (single sign on) for specific departments
- Review policies to address (in a timely manner) vulnerabilities, for each device to remediate identified problems;
- Review process for requesting vendors to provide the ability to identify user level database access and audit/ modification reports;
- Review solution options for technology to automatically identify and encrypt PHI in email or attachments, and
- Any other compliance-related assignments that your organization and ecfirst agree are a priority and fall within ecfirst's expertise.

On-Demand Compliance Solutions from ecfirst provides your organization with access to specialized compliance and security skills with no short term or long term commitments. Get Started Today!

Return to Table of Contents

Health IT Services

On-Demand through Managed Compliance

bizSHIELD tm

The HIPAA Academy offers the healthcare industry's most flexible range of Health Information Technology (IT) services. What's more is that the services are all based on flat rate pricing that get even more valued based on the duration of service provided. The Health IT service options available now are:

- On-Demand Consulting
- Managed Compliance Services Program (MCSP)

On-Demand Consulting, *You Can Do It, We Can Help!*

Starting with a commitment of 40-hours or more, you can secure IT professional resources with experience in the healthcare industry across a broad range of skill sets. So be with project management, security professionals, compliance professionals, system analysts, network engineers or more, talk to ecfirst about your requirements and how we can help with staffing or collaborating with you on your project initiatives under our management with your objectives.

We at ecfirst refer to this Health IT consulting model as – "*you can do it, we can help!*" ecfirst resources may be applied to work along with your personnel to help support, manage or implement IT solutions or capabilities. For example, ecfirst can support your activities with specialized resources such as:

- Project managers with experience as required
- Technical professionals with extensive technical, compliance or security expertise

The scope of work may be executed on-site, at your site, or offsite, as determined by your organization. Time-lines, reporting structure and frequency are mutually determined. A sampling of possible tasks and activities include:

- Develop and manage a Project Plan for IT project initiatives, such as Meaningful Use, or an EHR technology or application implementation.
- Perform Project Management duties and provide technical implementation assistance.
- Develop and manage policies to address proactive auditing.
- Deploy systems, applications or technologies.
- License assessment (software, application license audit).
- Develop a program, procedures, and logs to combine and filter audit logs, network activity review, and application security access reviews.
- Assist in developing Incident Management capabilities, policy, and technical procedures.
- Review solution options to encrypt sensitive information in email or portable devices.

Managed Compliance Services Program (MCSP)

We Get It Done!

The Managed Compliance Services Program (MCSP) is the industry's most unique and flexible managed services program. With the MCSP you decide what combination of services you contract with ecfirst to manage, and you determine the duration – one year, two years, three years or five years. The duration of the contract determines the flat rate discount you secure for the length of the contract. And, to top it, payments are monthly for the duration of the contract, with absolutely no interest, and nothing due upfront!

So you decide what service components are to be delivered by ecfirst in what timeframe*. It's amazingly, simple!*

For example, are your internal resources stretched to capacity and you lack the necessary expertise to identify all compliance gaps and security vulnerabilities? Does your organization need to comply with regulations and standards such as the HITECH Act, State Regulations, HIPAA Privacy and HIPAA Security?

Regulations mandate organizations to maintain compliance with reasonable and appropriate safeguards in several specific areas. Compliance requirements drive critical activities that must be conducted on a regular schedule, typically annually. On a regular schedule, organizations must by law:

- Assess compliance with the HIPAA, HITECH or state regulations.
- Assign responsibility to the security officer who is responsible for coordinating compliance and security initiatives.
- Conduct a comprehensive and thorough risk analysis including technical 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 the information infrastructure for compliance with the HIPAA Security Rule.

Program Benefits

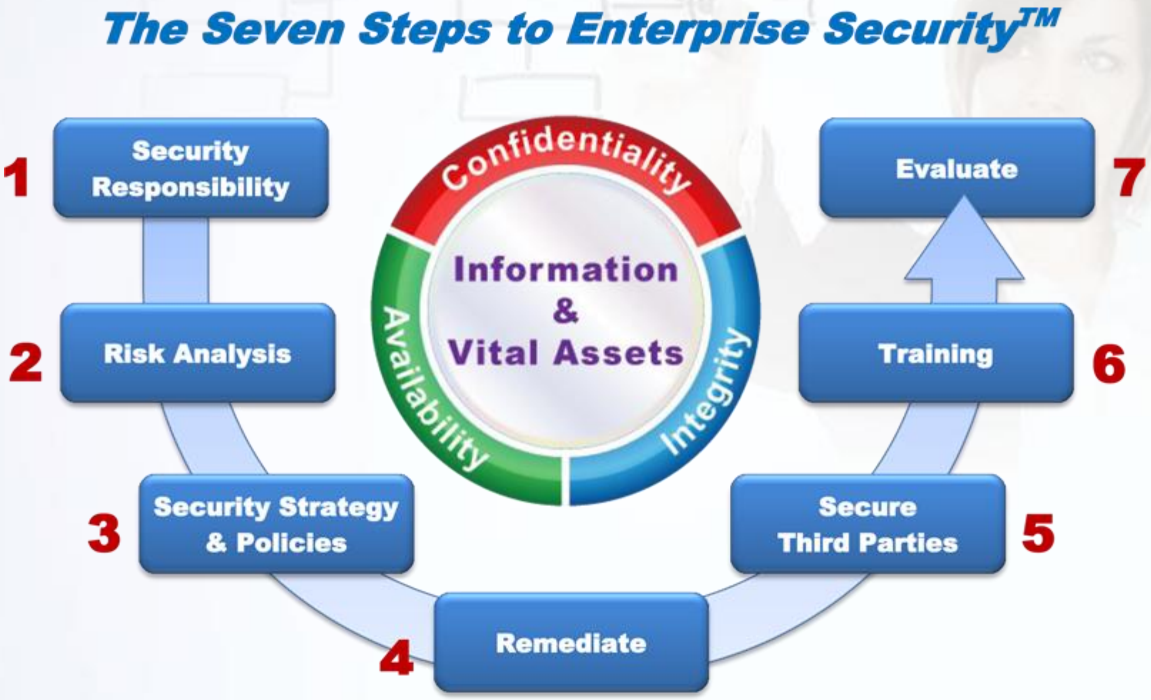
MCSP is designed to assist *healthcare organizations and business associates* manage compliance requirements, security and core components of the technology infrastructure. Key benefits of MCSP include:

- Clearly defined deliverables to achieve compliance.
- Expert advisor assigned – serves as interim security advisor.
- Activities such as risk analysis, technical vulnerability assessment 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 we focus on compliance.
- Fixed monthly fee.
- No interest.

Further benefits of the MCSP include:

- A team of experts keeps you up to date on regulations.
- We free up cycles to enable your staff to better focus on business-critical tasks.
- Depth in resource capabilities with trusted knowledge of legislation and client infrastructure.
- Smooth out volatility in resource demands and costs associated with managing information technology.
- ecfirst helps to minimize productivity losses from unexpected downtime.

This chart summarizes key areas addressed by the ecfirst MCSP.


The Seven Steps to Enterprise Security™
1 Security Responsibility
2 Risk Analysis
3 Security Strategy & Policies
4 Remediate
5 Secure Third Parties
6 Training
7 Evaluate
Confidentiality
Integrity
Availability
Information & Vital Assets

ecfirst*'s Managed Compliance Services Program (MCSP)*

The MCSP is designed to address your compliance, security and other technology implementation, support and management challenges. This program enables your organization to both lower costs and save time. The MCSP is a highly flexible and scalable service.

The MCSP provides *a complete, end-to-end compliance service offering* that can be tailored to meet your specific requirements.

Return to Table of Contents

Edit & Go^{TM} Policy Templates

HIPAA Privacy, HIPAA Security, HITECH, ISO 27000/2 & PCI DSS

bizSHIELD^{tm}

Cornerstone of Compliance Mandates Are Policies

Are your organizational privacy and information security policies updated to meet compliance mandates? Be it state (California, Massachusetts or over 40 others), federal (HIPAA Privacy, HIPAA Security, HITECH Act), Industry Standards such as PCI DSS or ISO 27000 – all require policies to be developed, approved and communicated to all members of the workforce!

Are your policies ready?

Already in use at hundreds of organizations, the ecfirst *biz*SHIELD^{tm} Policy Templates are the most complete in the industry. Any company or agency can easily tailor the policies – **Edit & Go^{TM}!**

HIPAA Privacy Policy Template Set

All covered entities are required to create HIPAA Privacy Policies as per the guidelines of HIPAA Privacy rule. Most of these policies are used in day to day administration.

“Essentially, a covered entity is required to develop and implement policies and procedures appropriate to the entity’s business practices and workforce that reasonably minimize the amount of protected health information used, disclosed, and requested.” (HIPAA Privacy Rule 45 CFR Part 160.)

Information Security Policy Template Set

The *biz*SHIELD^{tm} security methodology identifies seven critical steps for an organization to establish a comprehensive framework for defending sensitive business information electronic Protected Health Information (EPHI) and vital assets. It is a roadmap to safeguard not just your digital assets but the organization’s information infrastructure as a whole. The *biz*SHIELD^{tm} security methodology includes these vital and necessary HIPAA security policies, now available exclusively through ecfirst – Home of the HIPAA Academy.

The security policies have been customized to meet the specific requirements of the HIPAA Security Rule. Over 60 specific security policies are included in the package and address the HIPAA Security Rule Standards and associated implementation specifications. Additionally, several best practices policies are included with this set that goes above and beyond the HIPAA Security Rule requirements.

ISO 27000/2 Policy Template Set

Organizations are increasingly considering applying the family of ISO 27000 international security standards to comply with various U.S. federal and state regulations such as HIPAA, HITECH, as well as standards such as the PCI DSS. The ISO 27000 is a global standard that provides a comprehensive framework that organizations can adopt to address compliance requirements and establish a resilient information infrastructure.

The ecfirst ISO 27000/2 policy template is complete and comprehensive. The template may be used to jumpstart your efforts to adopt ISO 27000 as the framework for information security. To assist you with addressing HIPAA Security mandates in the ISO 27002 framework, we created a user-friendly reference matrix. This downloadable matrix is now available for purchase from our Online Store.

PCI DSS Policy Template Set

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.

The ecfirst PCI DSS policy templates are based upon the 12 requirements and the associated sub-requirements of the Data Security Standard. These policies are designed for use by any organization needing to comply with PCI DSS and are highly suitable to be tailored for broader information security policy mandates. These policies were meticulously designed by information security experts and can assist your organization in meeting the policy requirements of PCI and better securing your organization.

Quick Reference Cards

The ecfirst Quick Reference cards are a fast way to gain information about key regulations and standards. Be it HIPAA, HITECH or the ISO 27000 – you will find the ecfirst Quick Reference Cards to be a valuable and handy reference. All Reference Cards are available for download after purchase from our Online Store.

Return to Table of Contents

Enterprise Information (System) Security Plan

Is it ready? Has it been updated?

*biz*SHIELDtm

A Compliance Requirement

Compliance mandates require organizations to develop an enterprise system security plan. An enterprise system security plan is one of the items typically requested as part of an on-site investigation or a compliance audit.

ecfirst is focused in the area of cyber security and compliance and has deep experience enabling organizations comply with regulatory mandates and standards including HIPAA, HITECH, PCI DSS, ISO 27000, and more.

Client Testimonial

“ecfirst was engaged to develop a comprehensive enterprise information security plan. The process of development of the plan included interviews, review of critical documents, including policies and information related to security controls implemented.”

“The ecfirst Security Team was very responsive and tailored the information security plan to our specific requirements, including compliance mandates/standards such as HIPAA, HITECH, ISO 27002 and NIST SP 800-53. Work was professionally executed and of exceptional quality. ecfirst has worked hard to earn our confidence and our trust. We look forward to work with ecfirst again in the near future.”
Tom Brink, *Director IT Operations, HIPAA Security Officer*
Maricopa Integrated Health System

A Customized Enterprise Security Plan

ecfirst can develop a customized enterprise information security plan specific to your organization based on your security priorities and compliance mandates.

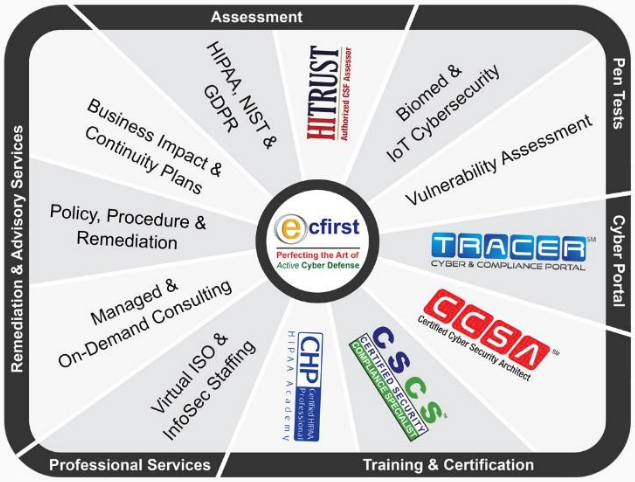
The ecfirst enterprise information security plan is based on the proprietary *biz*SHIELDtm methodology developed by ecfirst and influenced by standards that include NIST and the ISO 27000. This plan provides the foundation for your enterprise security policies and procedures. This plan must be aligned with your business objectives.

The ecfirst enterprise information security plan establishes the blueprint for your security and compliance priorities. Get this plan developed now and get ahead with your security initiatives and projects.

Return to Table of Contents

ecfirst

Perfecting the Art of *Active* Cyber Defense


Assessment
Pen Tests
Cyber Portal
Training & Certification
Professional Services
Remediation & Advisory Services
HIPAA, NIST & GDPR
HITRUST Authorized CSF Assessor
Biomed & IoT Cybersecurity
Vulnerability Assessment
TRACER SM CYBER & COMPLIANCE PORTAL
CCSA Certified Cyber Security Architect SM
CSCS Certified Security Compliance Specialist SM
CHP Certified HIPAA Professional HIPAA Academy
Virtual ISO & InfoSec Staffing
Managed & On-Demand Consulting
Policy, Procedure & Remediation
Business Impact & Continuity Plans
ecfirst Perfecting the Art of Active Cyber Defense

VISION (Mantra)

Enabling establishment of an active cyber defense program and capability.

MISSION (Karma)

Implement an evidence-based compliance program integrated within an enterprise-wide active cyber defense system.

OUR PROMISE

- Unconditional Guarantee. No Questions!
- ecfirst will not consider an engagement complete unless client is 100% satisfied.

Client Reference

“I just wanted to take a moment and say thank you. Thank you and the ***excellent team*** at ecfirst for ***hard work***, late hours and ***diligence*** during the first round of our HITRUST certification, and now working on our annual risk management and HIPAA compliance assessment.”

“From HIPAA compliance, cybersecurity pen tests, to the HITRUST certification engagement, we have found ecfirst to be an ***exceptional partner*** that labored incredibly hard for us, with us. The ecfirst insight and diligence to ensuring HITRUST certification mandates are met led to us completing our engagement on budget and time. We look forward to deeper collaboration with ecfirst in the cybersecurity space in the future. I continue to recommend ecfirst highly and often!”

BRG Berkeley Research Group

Chip Goodman | Vice President of Information Technology

“The ecfirst team literally helped us build our HIPAA practices from ground up since 2012, allowing us to offer secure HIPAA-compliant eHealth and health IT solutions to our customers across the U.S. We are actively taking the logical next step in working with ecfirst to pursue the HITRUST certification in order to further expand our market. We see the partnership with ecfirst as an ***integral part*** of our business strategy and have been ***extremely satisfied*** with the ***quality and value*** of the services that ecfirst has rendered.”

BrightOutcome COLLABORATIVE SYMPTOM MANAGEMENT

DerShung Yang | Founder & President

“Provant Health partnered with ecfirst to build a plan and assist in executing it with the goal of achieving HITRUST certification. Ali Pabrai and his team were ***flexible, collaborative*** and most importantly patient as we worked to educate our management team and key employees on the meaning and value of HITRUST. I’d recommend ecfirst to any company who wants to understand HITRUST or work on assessing and remediating their processes and systems in preparation for certification.”

provant health *life. changing.*

Tom Basiliere | Chief Information Officer

John Schelewitz | John.Schelewitz@ecfirst.com | +1.480.663.3225

Delivering Everything Compliance. Everything Security.

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

HITRUST Authorized CSF Assessor

ecfirst Perfecting the Art of *Active* **Cyber Defense**

HIPAA™ Academy

CSCS™ CERTIFIED SECURITY COMPLIANCE SPECIALIST

CHP Certified HIPAA Professional HIPAA Academy

TRACER℠ CYBER & COMPLIANCE PORTAL

CCSA℠ Certified Cyber Security Architect

ziksaka An E-Learning Portal

my ecfirst

HITRUST Authorized CSF Assessor

Corporate Office

295 NE Venture Drive
Waukee, IA 50263
United States

John T. Schelewitz

Director of Sales
ecfirst/HIPAA Academy
Phone: +1.480.663.3225
Email: John.Schelewitz@ecfirst.com
www.ecfirst.com