Compliance Mandates Require Technical Vulnerability Assessment

A key requirement of compliance mandates & security standards such as ISO 27000, HIPAA, PCI DSS & others is that organizations must conduct a comprehensive & thorough assessment of the potential risks & vulnerabilities to the confidentiality, integrity, & availability (CIA) of all sensitive, confidential information. These mandates require that organizations must complete a comprehensive & thorough vulnerability assessment on a regular schedule.

**bizSHIELDtm** – An ecfirst Technical Vulnerability Assessment Service

ecfirst developed the bizSHIELDtm program to assist organizations in addressing the requirements of compliance mandates & all subsequent guidance documentation & settlement agreements.

As a part of the bizSHIELDtm program, ecfirst identifies vulnerabilities from the outside (external) & inside (internal) the organization. Next, ecfirst develops recommended remediation activity, & associated risk priority. All remediation activities will be listed according to recommended implementation time bands in the bizSHIELDtm Corrective Action Plan (CAP) table. The bizSHIELDtm report is an actionable, documented risk analysis that provides both in depth & executive summary level findings appropriate to all audiences from administrators to the Board of Directors.

Technical Vulnerability Assessment & Penetration Test

Among the items that may be requested as part of a HIPAA compliance audit or an investigation is a copy of the latest vulnerability assessment report. The vulnerability assessment report provides information on risks associated with security gaps that may be exploited to compromise the confidentiality, integrity, &/or availability of Electronic Protected Health Information (EPHI) or other such confidential information such as Personally Identifiable Information (PII).

The ecfirst Platinum Technical Vulnerability Assessment is comprehensive in scope as it addresses both external & internal vulnerabilities. A detailed technical Corrective Action Plan (CAP) is included in the bizSHIELDtm report to provide actionable directives for addressing the identified deficiencies.
Technical Vulnerability Assessment vs. Penetration Test

ecfirst’s Technical Vulnerability Assessment (TVA) & Penetration Test (PT) both identify vulnerabilities within your network & provide a report enumerating the issues discovered as well as recommendations for remediation. The main difference between the two is the focus: a TVA’s focus is to identify all vulnerabilities & deviations from best practice that create a risk, while a PT’s focus is to demonstrate that risk.

A PT has a goal, such as ‘Obtain EPHI’, & demonstrates the risk of not remediating identified vulnerabilities by utilizing them to reach this goal. The TVA only looks to identify vulnerabilities, while the PT actually tries to EXPLOIT those vulnerabilities. Unless you already have a robust & mature security program in place, most organizations are best served by performing a Technical Vulnerability Assessment(s) prior to Penetration Testing activities.

Technical Vulnerability Assessment Service

The ecfirst bizSHIELD™ risk analysis program includes a technical vulnerability assessment to address compliance mandates with the objective of establishing & prioritizing compliance & security gaps. The ecfirst bizSHIELD™ Technical Vulnerability Assessment Service supports several distinct components, including:

- External Assessment
- Internal Assessment
- Firewall Assessment
- Wireless Assessment
- Social Engineering Assessment
The following are the brief stages involved in the assessment:

- Scope & preparation
- Discovery & vulnerability analysis
- Exploitation (penetration tests only), &
- Reporting & documentation

A subset of systems will be identified as **in-scope** for both the external & internal networks as applicable; these are the systems that will be scanned/tested. The objective of the vulnerability assessment is to identify potential security risks & vulnerabilities within these **in-scope systems**.

Data gathered is analyzed against policies, HIPAA regulations, standard best practices, & vendor security bulletins in order to determine potential risks & exposures to the computing environment. The results of these vulnerability scans/tests are to be used as the basis for determining the security posture & risk of other systems not directly tested.

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

The ecfirst Titanium Vulnerability Assessment is broken up into four (4) distinct areas of analysis performed entirely remotely:

*Note: You must be able to deploy a Virtual Machine image (in OVF format) supporting our defined specifications, such as an ESX server or VMWare Workstation installation. If you are unable to deploy our Virtual Machine image, we will have to send you a hardware device at an additional cost*

- **External Assessment** - to be mutually determined & performed remotely
  - Externally accessible IP addresses (up to 256) are scanned for vulnerabilities
    - All identified vulnerabilities are validated to the extent possible
  - Up to four (4) external domains are tested for:
    - Google Hacking Database (GHDB) entries
    - DNS misconfigurations
    - Metadata in publicly accessible documents, &
  - Up to two (2) websites/applications are crawled/scanned for vulnerabilities under one (1) user role

- **Internal Assessment** - to be mutually determined & performed remotely
  - Internal IP addresses (up to 4096) are scanned for vulnerabilities
    - All identified vulnerabilities are validated to the extent possible
  - Up to 16 Class C network ranges are scanned for
    - Devices responding to “default” SNMP Community Strings
    - Systems running up to three (3) database server types (i.e. MSSQL, MySQL, Oracle, etc.) that allow open access, &
      - Identified systems are also tested for “default” credentials
  - Up to three (3) Active Directory domains are tested for:
    - Identity & Access Management (IAM) best practice adherence
    - Password Policy best practice adherence
    - User account password strength, &
    - USB device enumeration of systems registered in Active Directory (AD)
      - Identification of currently connected devices

- **Firewall Assessment** - to be mutually determined & performed remotely
  - Firewall configurations to identify OS
    - The firewall rules on one (1) device
Wireless Assessment (performed remotely)
  - **ecfirst** will send you a handheld device (along with instructions) that someone in your organization will utilize to assist **ecfirst** in this portion of the assessment
  - Assessment of the Organization to identify:
    - Potentially rogue Access Points/SSIDs
    - Open wireless access segmentation review, &
      - Includes testing of segmentation
    - Insecure authentication/encryption configurations
      - Includes testing of Pre-shared Key (PSK) strength

**ecfirst** documents all security issues found in the *bizSHIELD™* report. In addition to including the findings & the Corrective Action Plan (CAP), the *bizSHIELD™* report also contains an Executive Action Plan (EAP) that outlines achievable goals & milestone dates for management or executive attention.

The EAP & CAP can be made available in a Microsoft Excel spreadsheet format so as to assist in importing the findings into a project management tool of their choice.
The ecfirst Platinum Vulnerability Assessment is broken up into four (4) distinct areas of analysis performed entirely remotely:

*Note: You must be able to deploy a Virtual Machine image (in OVF format) supporting our defined specifications, such as an ESX server or VMWare Workstation installation. If you are unable to deploy our Virtual Machine image, we will have to send you a hardware device at an additional cost*

- **External Assessment (performed remotely)**
  - Up to Sixteen (16) externally accessible IP addresses are scanned for vulnerabilities
    - All identified vulnerabilities are validated to the extent possible
  - Up to three (3) external domains are tested for:
    - Google Hacking Database (GHDB) entries
    - DNS misconfigurations
    - Metadata in publicly accessible documents, &
  - Up to two (2) websites/applications are crawled/scanned for vulnerabilities under one (1) user role

- **Internal Assessment (performed remotely)**
  - Up to Sixteen (16) Internal IP addresses are scanned for vulnerabilities
    - All identified vulnerabilities are validated to the extent possible
  - Up to three (3) Class C network ranges are scanned for
    - Devices responding to “default” SNMP Community Strings
    - Systems running up to three (3) database server types (i.e. MSSQL, MySQL, Oracle, etc.) that allow open access, &
      - Identified systems are also tested for “default” credentials
  - Up to two (2) Active Directory domains are tested for:
    - Identity & Access Management (IAM) best practice adherence
    - Password Policy best practice adherence
    - User account password strength, &
    - USB device enumeration of systems registered in Active Directory (AD)
      - Identification of currently connected devices

- **Firewall Assessment (performed remotely)**
  - Firewall configurations to identify OS
• Wireless Assessment (performed remotely)
  o ecfirst will send you a handheld device (along with instructions) that someone in your organization will utilize to assist ecfirst in this portion of the assessment
  o Assessment of one (1) physical building to identify:
     ▪ Potentially rogue Access Points/SSIDs
     ▪ Open wireless access segmentation review, &
       • Includes testing of segmentation
     ▪ Insecure authentication/encryption configurations
       • Includes a Determination of the Pre-shared Key (PSK) strength

ecfirst documents all security issues found in the bizSHIELD™ report. In addition to including the findings & the Corrective Action Plan (CAP), the bizSHIELD™ report also contains an Executive Action Plan (EAP) that outlines achievable goals & milestone dates for management or executive attention.

The EAP & CAP can be made available in a Microsoft Excel spreadsheet format so as to assist in importing the findings into a project management tool of their choice.
The ecfirst Gold Vulnerability Assessment is broken up into three (3) distinct areas of analysis performed entirely remotely:

**Note: You must be able to deploy a Virtual Machine image (in OVF format) supporting our defined specifications, such as an ESX server or VMWare Workstation installation. If you are unable to deploy our Virtual Machine image, we will have to send you a hardware device at an additional cost**

- **External Assessment (performed remotely)**
  - Up to eight (8) externally accessible IP addresses are scanned for vulnerabilities
  - One (1) external domain tested for:
    - Google Hacking Database (GHDB) entries
    - DNS misconfigurations
    - Metadata in publicly accessible documents
  - One (1) website/application anonymously crawled/scanned for vulnerabilities

- **Internal Assessment (performed remotely)**
  - Up to eight (8) internal IP addresses are scanned for vulnerabilities
  - One (1) Class C network range scanned for:
    - Devices responding to “default” SNMP Community Strings, &
    - Systems running one (1) database server type (i.e. MSSQL, MySQL, etc.) that allow open access, &
      - Systems also tested for “default” credentials
  - One (1) Active Directory domain tested for:
    - Identity & Access Management (IAM) best practice adherence
    - Password Policy best practice adherence
    - User account password strength, &
    - USB device enumeration of systems registered in Active Directory (AD)

- **Firewall Assessment (performed remotely)**
  - Firewall configuration to identify OS

ecfirst documents all security issues found in the bizSHIELD™ report. In addition to including the findings & the Corrective Action Plan (CAP), the bizSHIELD™ report also contains an Executive Action Plan (EAP) that outlines achievable goals & milestone dates for management or executive attention.

The EAP & CAP can be made available in a Microsoft Excel spreadsheet format so as to assist in importing the findings into a project management tool of their choice.
The ecfirst Silver Vulnerability Assessment is broken up into two (2) distinct areas of analysis performed entirely remotely:

- **External Assessment (performed remotely)**
  - Up to eight (8) externally accessible IP addresses are scanned for vulnerabilities
  - One (1) external domain tested for:
    - Google Hacking Database (GHDB) entries
    - DNS misconfigurations
    - Metadata in publicly accessible documents,
  - One (1) website/application anonymously crawled/scanned for vulnerabilities

- **Firewall Assessment (performed remotely)**
  - Firewall configuration to identify OS

It should be noted that the ecfirst Silver Level Vulnerability Assessment would most likely not be considered a comprehensive vulnerability assessment, as critical areas related to the internal network/system management are not included in the testing.

ecfirst documents all security issues found in the bizSHIELD™ report. In addition to including the findings & the Corrective Action Plan (CAP), the bizSHIELD™ report also contains an Executive Action Plan (EAP) that outlines achievable goals & milestone dates for management or executive attention.

The EAP & CAP can be made available in a Microsoft Excel spreadsheet format so as to assist in importing the findings into a project management tool of their choice.
Bronze Vulnerability Assessment

The ecfirst Bronze Vulnerability Assessment consists of one (1) area of testing & is performed entirely remotely:

- External Assessment (performed remotely)
  - Up to five (5) externally accessible IP addresses are scanned for vulnerabilities, &
  - One (1) website/application anonymously crawled/scanned for vulnerabilities

Only the “raw” results of the tests performed are provided in the Bronze Vulnerability Assessment report. Unlike the bizSHIELD™ report, ecfirst does not perform any additional analysis & as such ecfirst does not provide a Corrective Action Plan (CAP), Executive Action Plan (EAP), Executive Summary, or detailed remediation steps.

It should be noted that the ecfirst Bronze Level Vulnerability Assessment would most likely not be considered a comprehensive vulnerability assessment, as critical areas related to the internal network/system management are not included in the testing.
Vulnerability Assessment Process

1. SOW Contract Executed
2. Kick Off Meeting
3. Data Collection Form
4. Data Collection Analysis
5. External Assessment
6. Internal Assessment
7. Report Creation
8. Compliance Analysis
9. Review & QA
10. Report Delivery
11. Executive Briefing
12. Remediation

Client & ecfirst  ecfirst  Client
The ecfirst External Penetration Test (performed remotely) includes the following specific items:

- The External Penetration Test is “pre-scoped” to the following general criteria
  - A “grey box” test is based on the following information provided
    - IP address ranges owned/operated &
    - All domains owned/associated with up to sixteen (16) external systems included in the scope

- The primary goal is to gain unauthorized elevated access to an externally accessible system
  - A secondary goal is to gain unauthorized access to other systems utilizing the primary goal system

- Out-of-Scope
  - End-user attacks (i.e. phishing, man-in-the-middle, client-side exploitation, etc.)
  - Denial of Service (DoS) attacks

The External Penetration Test methodology is described below:

- **Reconnaissance**
  - Client personnel & cultural information
  - Client business terminology
  - Technical infrastructure information

- **Scanning**
  - Network Discovery
  - Network Port & Service Identification
  - Vulnerability Identification
  - Wireless LAN Discovery/Scanning
  - Enumeration

- **Exploitation**
  - Password cracking
  - Discovered credential usage
  - Manual & Automated vulnerability validation
  - Privilege escalation
  - Additional tool installation
  - Data discovery
Obtain EPHI/PII

Compromise an external system containing EPHI/PII
- ecfirst External Penetration
- Compromise an external system
- ecfirst External Penetration
- Gain remote network access
  - ecfirst External Penetration
  - ecfirst Social Engineering "out of scope"
- Compromise a client system

Compromise an internal system
- Gain internal network access
  - ecfirst Internal Penetration
  - ecfirst Physical Penetration "out of scope"
  - ecfirst Social Engineering "out of scope"
Internal Penetration Test

The ecfirst Internal Penetration Test (performed remotely) includes the following specific items:

- The Internal Penetration Test is “pre-scoped” to the following general criteria:
  - A “grey box” test is based on the following information provided
    - Domain User account configured as a “regular” employee
    - Remote access to the internal network via a Virtual Machine or physical device ecfirst provides
  - Not all vulnerabilities identified will be validated &/or exploited
    - Only those deemed most likely to assist in reaching the defined Goal will be further validated & exploited
- The primary goal is to gain Domain Administrator level access on the internal network
  - A secondary goal is to gain unauthorized access to sensitive data
- Out-of-Scope
  - End-user attacks (i.e. phishing, man-in-the-middle, client-side exploitation, etc.)
  - Denial of Service (DoS) attacks

The Internal Penetration Test methodology is described below:

- Scanning
  - Network Discovery
  - Network Port & Service Identification
  - Vulnerability Identification
  - Wireless LAN Discovery/Scanning
  - Enumeration
- Exploitation
  - Password cracking
  - Discovered credential usage
  - Manual & Automated vulnerability validation
  - Privilege escalation
  - Additional tool installation
  - Data discovery
Obtain EPHI/PII

Compromise an Internal system containing EPHI/PII
- ecfirst Internal Penetration

Compromise an internal system
- ecfirst Internal Penetration
- ecfirst Social Engineering "out of scope"

Gain internal network access
- ecfirst Internal Penetration
- ecfirst Physical Penetration "out of scope"

Compromise a client system
- ecfirst Social Engineering "out of scope"
Web Application Penetration Test

The scope of a Web application penetration test includes the following specific items:

- One (1) Web Application to be assessed
- One (1) user role type to be utilized for testing
  - “Client” user account type
  - Anonymous access will also be tested
- General Goal(s)
  - Gain anonymous access to authenticated sections of the application
  - Gain access to other client data within the application
- Out-of-scope
  - Underlying System vulnerability exploitation
  - System Account Creation
  - Web Application Firewall (WAF) &/or IDS/IPS evasion

The Web Application Penetration Test methodology is described below:

**Reconnaissance**

- Client personnel & cultural information
- Client business terminology
- Technical infrastructure information

**Mapping**

- Network Discovery
- Network Port & Service Identification
- Analyzing HTTPS Support
- Identify Virtual Hosting & Load Balancers
- Analyze Software Configuration
- Spider the site/application
- Application flow charting
- Relationship analysis
- Session analysis

**Discovery**

- Automated Vulnerability Scanning
- Information Leakage & Directory Browsing Discovery
- Username Harvesting & Password Guessing
- Command Injection Discovery
- Directory Traversal & File Inclusion Discovery
- SQL Injection Discovery
- Cross-site Scripting (CSS) Discovery
- Cross-site Request Forgery (CSRF) Discovery
- Session Flaw Discovery
- Insecure Redirects & Forwards Discovery

**Exploitation**

- Exploit identified Enumeration flaws
- Exploit identified Bypass flaws
- Exploit identified Injection flaws
- Exploit identified Session flaws
- Chain exploits together, pivot to other systems, data exfiltration, raid the fridge, etc
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 & 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 & 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, & procedural controls during this assessment. ecfirst will document & present a very detailed record of successes, failures, controls bypassed, access achieved & information obtained during the assessment.

Client Testimonial

“ecfirst provides excellent value across a comprehensive portfolio of first rate solutions for regulations such as HIPAA | HITECH compliance, risk analysis, social engineering, vulnerability assessment, disaster recovery and business continuity. They are not just experts in these respective fields but are able to communicate & motivate corporate audiences to effect change.”

“ecfirst is an excellent business partner that focuses on long term, successful relationships through consistently successful project delivery.”

Joe Granneman, CTO & CSO, Rockford Health System
ecfirst Facts

- Established in 1999
- Clients in all 50 U.S. States
- Global experience includes Philippines, India, Middle-East, Canada, Africa
- Industry experience includes healthcare, IT, finance, government, and legal
- Privately held
- Unconditional guarantee for services delivered

Security Risk Assessment

Conduct a comprehensive risk assessment to identify compliance gaps and security vulnerabilities. Services also include vulnerability assessment and penetration testing.

On-Demand Consulting

Immediately add resources, off-site or on-site, to jumpstart compliance and security projects. Flat rate pricing.

Managed Compliance. Managed Security

Fixed monthly fee for a one, two, three, or five year period to manage compliance and information security projects. Includes security risk assessments, policy/procedure development, training, consulting, remediation, certification and more.

HITRUST Assessment & Certification

Jump-start your requirements to address the HITRUST CSF requirements with specialized ecfirst solutions for self-assessment, validation, and certification. With knowledge transfer every step of the way, ecfirst is positioned to be your trusted partner to manage HITRUST CSF assessments, including certification. ecfirst is a PCI QSA.

Client Testimonials

"Nixon Peabody retained the services of Ali Pabrai, MSE, CissP as an expert in information security. Found Mr. Pabrai and his firm, ecfirst, as exceptionally responsive in supporting all our activities as requested on a timely and professional manner. His insight was valued and of significance."

Linn F. Freedman, Partner
Nixon Peabody LLP

"Prime Healthcare and its network of 40+ hospitals is excited to have partnered with an organization - ecfirst - that is recognized in the healthcare industry as a leader devoted to enabling health systems to continually address information privacy and security regulatory requirements."

Prime Corp.

"ecfirst has demonstrated dedication to ensuring that project goals were met or exceeded every step of the way. I strongly recommend ecfirst to anyone in need of similar services."

Doug Springmeyer
State of Utah, Attorney General's Office

Training & Certification

CHA
Certified HIPAA Professional
HIPAA Academy

Fast track program for end users to learn the basics of HIPAA and HITECH regulations, including the HIPAA Privacy Rule.

CHP
Certified HIPAA Professional
HIPAA Academy

Industry’s first & most comprehensive program on HIPAA and HITECH. Covers everything HIPAA, including Transactions, Code Sets, Privacy, Security and Breach Notification.

CSCS
Certified Security Compliance Specialist

World’s first program focused on compliance regulations and cyber security. Covers ISO 27001, PCI DSS, NIST, FISMA, HIPAA and more.

CCSA
Certified Cyber Security Architect

First executive training program designed to enable development of a cyber security program in the class.

ISO 27000 Workshop

In-depth review of ISO 27000, 27001 & 27002.

Complimentary Brief! Schedule Today.

Karen Durbin | +1.515.444.1221 | Karen.Durbin@ecfirst.com
Lorna Waggoner | +1.515.779.6629 | Lorna.Waggoner@ecfirst.com
Adam Romo | +1.714.258.6928 | Adam.Romo@ecfirst.com

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

HITRUST
Authorized CSF Assessor
PCI Security Standards Council
