Applying ISO 27000 and NIST to Address Compliance Mandates

The Four Laws of Information Security

Ali Pabrai, **MSEE, CISSP (ISSAP, ISSMP)**
ecfirst, chief executive
Member, FBI InfraGard

Challenges

PHI Is @ Significant Risk!

- **Healthcare - Complex Computing Environment**
  - ❑ Too many servers, too many applications
  - ❑ Too many credentials across multiple systems to manage
  - ❑ Too many end systems to support and maintain
  - ❑ Mobility of devices is rapidly increasing
  - ❑ Storage demands are rising fast
  - ❑ Highly specialized technical skills required
  - ❑ Serious lack of redundancy in infrastructure
  - ❑ Struggle with resources to monitor and audit
- **Security**
  - ❑ Struggling with fast, secure access to patient information
  - ❑ Generic accounts still in active use
  - ❑ Struggling with password management
  - ❑ Need to uniquely identify “who accessed what, when, how”
  - ❑ Audit controls are not consolidated not automated; not complete

Breach Reports - OCR

1. State: Tennessee
   Approx. # of Individuals Affected: 1,711
   Date of Breach: 7/15/10
   Type of Breach: Loss
   Location of Breached Information: Portable Electronic Device, Other

2. State: Ohio
   Approx. # of Individuals Affected: 13, 867
   Date of Breach: 6/7/10
   Type of Breach: Theft
   Location of Breached Information: Laptop

3. State: Illinois
   Approx. # of Individuals Affected: 657
   Date of Breach: 6/5/10
   Type of Breach: Theft, Loss
   Location of Breached Information: Paper Records

4. State: Texas
   Approx. # of Individuals Affected: 600
   Date of Breach: 5/29/10
   Type of Breach: Theft
   Location of Breached Information: Network Server

5. State: Arizona
   Approx. # of Individuals Affected: 5,893
   Date of Breach: 5/15/10
   Type of Breach: Theft
   Location of Breached Information: Laptop

6. State: Michigan
   Approx. # of Individuals Affected: 2,300
   Date of Breach: 5/02/10
   Type of Breach: Theft
   Location of Breached Information: Laptop

Breaches in CA – OCR

1. Loma Linda University School of Dentistry
   Approx. # of Individuals Affected: 10,100
   Date of Breach: 6/13/10
   Type of Breach: Theft
   Location of Breached Information: Desktop Computer

2. Children's Hospital & Research Center at Oakland
   Approx. # of Individuals Affected: 1,000
   Date of Breach: 5/25/10 and 5/26/2010
   Type of Breach: Other
   Location of Breached Information: Paper

3. Loma Linda University Health Care
   Approx. # of Individuals Affected: 584
   Date of Breach: 4/04/10
   Type of Breach: Theft
   Location of Breached Information: Desktop Computer

4. Silicon Valley Eyecare Optometry and Contact Lenses
   Approx. # of Individuals Affected: 40,000
   Date of Breach: 4/02/10
   Type of Breach: Theft
   Location of Breached Information: Network Server

5. St. Joseph Heritage Healthcare
   Approx. # of Individuals Affected: 22,012
   Date of Breach: 3/06/10
   Type of Breach: Theft
   Location of Breached Information: Desktop Computer

6. John Muir Physician Network
   Approx. # of Individuals Affected: 5,450
   Date of Breach: 2/04/10
   Type of Breach: Theft
   Location of Breached Information: Laptop

Compliance Mandates

- Key Regulations & Standards
  - HIPAA Privacy
  - HIPAA Security
  - HITECH Act
  - FACTA (Red Flags Rule)
  - State Regulations
  - PCI DSS

Meaningful Use

Stage 1 Core Set Mandate

- Ensure adequate privacy and security protections for personal health information
  - Through use of policies, procedures, and technologies
- Meaningful Use Stage 1 Objective (Final Rule)
  - Protect EHR created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities
- Meaningful Use Stage 1 Measure (Final Rule)
  - *Conduct or review a security risk analysis and implement security updates as necessary and correct identified security deficiencies as part of the risk management process*

Massachusetts 201 CMR 17.00

Comprehensive Written Information Security Program Required

- Establishes minimal standards for safeguarding personal information contained in both paper and electronic records
- Requires each covered business to “develop, implement, maintain and monitor a comprehensive written information security program” that applies to records that contain Massachusetts’ residents’ personal information
- Security program must include “administrative, technical and physical safeguards” to protect such records
- Regulations also require businesses that store or transmit personal information about Massachusetts’ residents to (201 CMR 17.04):
  - ❑ Restrict access by use of passwords
  - ❑ Deploy updated malware protection
  - ❑ Encrypt information transmitted across public or wireless networks
  - ❑ Monitor all systems to detect unauthorized access
  - ❑ Encrypt information stored on laptops
  - ❑ Incorporate firewalls

State of Connecticut
IC-25

- All insurance companies doing business in Connecticut must report information breaches to state authorities within five calendar days, even if the data involved was encrypted
- The new state insurance breach reporting policy applies to health maintenance organizations, preferred provider organizations, and other health insurers, as well as property and casualty insurers, pharmacy benefit managers and medical discount plans
  - It does not apply to hospitals and physicians
  - A tough regulation which applies to paper and electronic records

PCI DSS

A Global Data Security Standard

A Terrific Reference Even If Your Organization is Not Required to Comply

1. **Build and Maintain a Secure Network**
   1. Firewall configuration
   2. Vendor defaults
2. **Protect Cardholder Data**
   3. Protect stored cardholder data
   4. Encrypt transmission
3. **Maintain a Vulnerability Management Program**
   5. Update anti-virus software
   6. Maintain secure systems and applications
4. **Implement Strong Access Control Measures**
   7. Restrict access – need to know
   8. Assign unique ID’s
   9. Restrict physical access
5. **Regularly Monitor and Test Networks**
   10. Track and monitor all access
   11. Regularly test security processes
6. **Maintain an Information Security Policy**
   12. Maintain policies

ISO 27000: An International Security Standard

- A comprehensive set of controls comprising best practices in information security
- Comprised of:
  - A code of practice
  - A specification for an information security management system
- Intended to serve as a single reference point for identifying a range of controls needed for most situations where information systems are used in industry and commerce

Organizations are looking at the ISO 27000 as a security framework to address HIPAA, HITECH, PCI DSS, State mandates

Process Approach

- ISO 27001 adopts the “Plan-Do-Check-Act” (PDCA) model

  A) **Plan** - Understanding an organization’s information security requirements and the need to establish policy and objectives for information security

  B) **Do** - Implementing and operating controls to manage an organization’s information security risks in the context of the organization’s overall business risks

  C) **Check** - Monitoring and reviewing the performance and effectiveness of the ISMS

  D) **Act** - Continual improvement based on the objective measurement

Application

- ISO 27001 covers all types of organizations
  - The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size, and nature
  - Can easily adapt to be organization-specific
- The ISMS for any organization is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to all interested parties

ISO 27002 Security Clauses

0. Risk Assessment & Treatment (Introductory Clause)
1. Security Policy
2. Organization of Information Security
3. Asset Management
4. Human Resources Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Information Systems Acquisition, Development and Maintenance
9. Information Security Incident Management
10. Business Continuity Management
11. Compliance

Risk Assessment & Treatment *Introductory Clause 0 (4)*

- The information security risk assessment should have a clearly defined scope in order to be effective
- The results should guide and determine appropriate management action and priorities for managing risks and for implementing controls selected to protect against these risks
- Consists of two categories:
  - ❑ Assessing Security Risks
  - ❑ Treating Security Risks

Assessing Security Risks

Category (4.1)

- Risk assessment should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization
  - A systematic approach of estimating the magnitude of risks (*risk analysis*)
  - The process of comparing the estimated risks against risk criteria to determine the significance of the risks (*risk evaluation*)
- For each risk identified, a risk treatment decision needs to be made

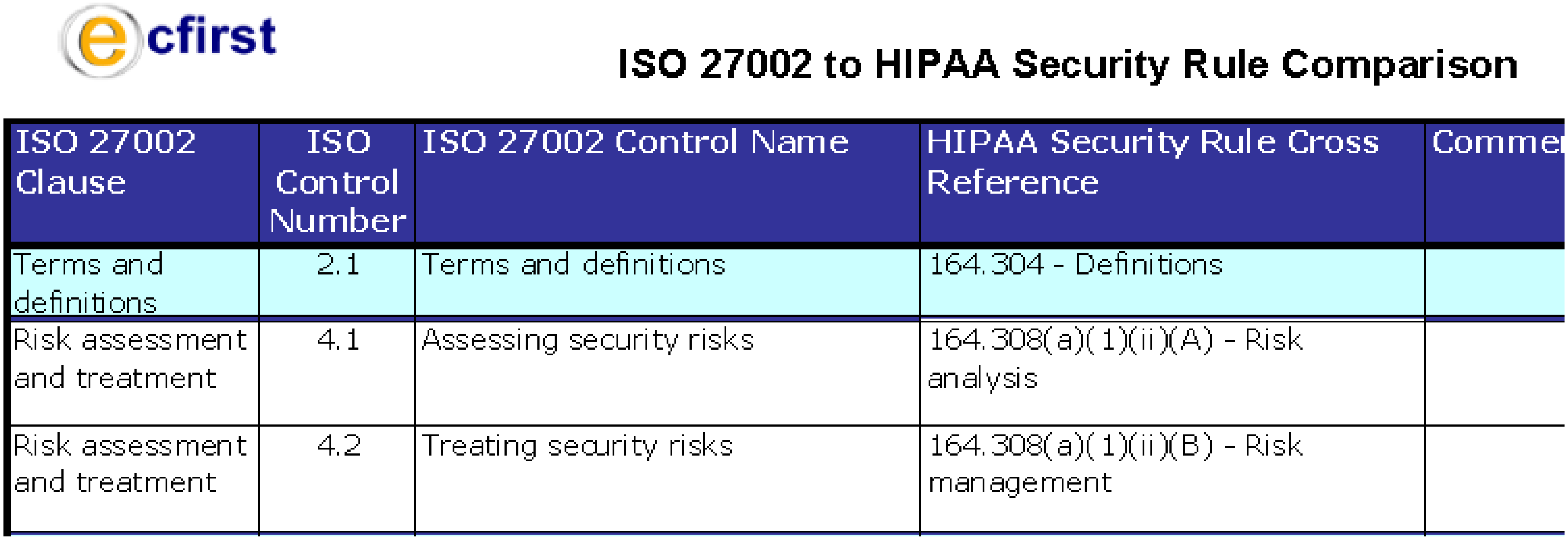
Treating Security Risks

Category (4.2)

- Possible options for <u>risk treatment</u> include:
  a) Applying appropriate controls to reduce the risks
  b) Knowingly and objectively accepting risks, providing they clearly satisfy the organization’s policy and criteria for risk acceptance
  c) Avoiding risks by not allowing actions that would cause the risks to occur
  d) Transferring the associated risks to other parties, e.g. insurance or suppliers

Risk Assessment & Treatment

Introductory Clause 0 (4)



ISO 27002 to HIPAA Security Rule Comparison

ISO 27002 Clause	ISO Control Number	ISO 27002 Control Name	HIPAA Security Rule Cross Reference	Comme
Terms and definitions	2.1	Terms and definitions	164.304 - Definitions	
Risk assessment and treatment	4.1	Assessing security risks	164.308(a)(1)(ii)(A) - Risk analysis	
Risk assessment and treatment	4.2	Treating security risks	164.308(a)(1)(ii)(B) - Risk management	

Security Policy
Clause 1 (5)

- Establishes the “dial-tone” for security in the organization
- Critical elements include:
  - Establishing management direction for information security
  - Regular updates and reviews
- Consists of 1 category
  - Information Security Policy (5.1)

Information Security Incident Management

Clause 9 (13)

- This clause provides guidance for the development and maintenance of a comprehensive strategy for responding to a security violation
- Consists of two categories:
  - ❑ Reporting Information Security Events and Weaknesses
  - ❑ Management of Information Security Incidents and Improvements

Business Continuity Management

Clause 10 (14)

- This clause provides guidance for the development and implementation of a comprehensive strategy to ensure continued business operation in the event of a catastrophic failure of systems of facilities
- Key parts of a comprehensive strategy include:
  - Procedures for failover to backup systems
  - Recovery of failed systems
  - Relocation of workforce members to alternate locations
- The only category defined in this clause is:
  1. Information Security Aspects of Business Continuity Management

ISO 27799

Health Informatics: Information Security Management in Health Using ISO 27002

- Defines guidelines to support the interpretation and implementation in health informatics of ISO 27002 and is a companion to that standard
- ISO 27799 specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines
- By implementing the ISO 27799, healthcare organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity and availability of personal health information

NIST

NIST SP 800-66 Rev 1 Is A Valuable Reference

The National Institute of Standards & Technology (NIST) has a critical role to play in ensuring federal agencies comply with FISMA

The NIST's FISMA-related responsibilities are:

- ❑ Development of standards, guidelines and associated methods and techniques
- ❑ Development of standards and guidelines, including establishment of minimum requirements for information systems
- ❑ Development of standards and guidelines for providing adequate information for all agency operations & assets

NIST 800-37 Rev 1

- Developed by NIST to comply with FISMA responsibility
- *Guide for Security Authorization of Federal Information Systems (NIST SP 800-37 Rev 1)*
  - ❑ *A Security Life Cycle Approach*
- A common *security authorization process* for federal information systems
- A well-defined and comprehensive security authorization process that helps ensure appropriate entities are assigned *responsibility and are accountable for managing information system-related security risks*

FIPS 199

- FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security
  - Breach of security is loss of confidentiality, integrity or availability
- The three levels of potential impact are:
  - Low
  - Moderate
  - High
- **FIPS 199 is the standard to categorize information and information systems**

FIPS 200

- FIPS 200 establishes the minimum security requirements for federal information and information systems
- This standard establishes the minimal requirements in eighteen security-related areas
- Federal agencies are required to meet the minimal requirements through the use of security controls in accordance with NIST SP 800-53
- **FIPS 199 and FIPS 200 are the first of two mandatory standards required by the FISMA legislation**

NIST SP 800-34

Contingency Planning

1. Develop a Contingency Planning Policy
2. Conduct Business Impact Analysis (BIA)
3. Identify preventative measures
4. Develop recovery strategy
5. Develop the Contingency Plan
6. Conduct testing and training
7. Review and maintenance

Contingency Plan – A HIPAA Security Rule Standard
Organizations are struggling to address!

NIST SP 800-111

Storage Encryption for End Devices

1. Develop comprehensive policy and conduct training
2. Consider solutions that use existing capabilities
3. Securely store and manage all keys
4. Select appropriate authenticators
5. Implement additional controls as needed

Centralize the Deployment of Storage Encryption!

NIST SP 122 - It's About PII.

Personally Identifiable Information

Until now, it has been about

- Protected Health Information (PHI) – *HIPAA Privacy*
- Electronic Protected Health Information (EPHI) – *HIPAA Security*
- Unsecured PHI – *HITECH Act*
- Cardholder information – *PCI DSS*
- Personal data or information – *State Regulations*

2010 and beyond – it is about PII

- What PII does your organization come into contact with?
- Where is PII in your organization?
- How is the PII secured in your organization?

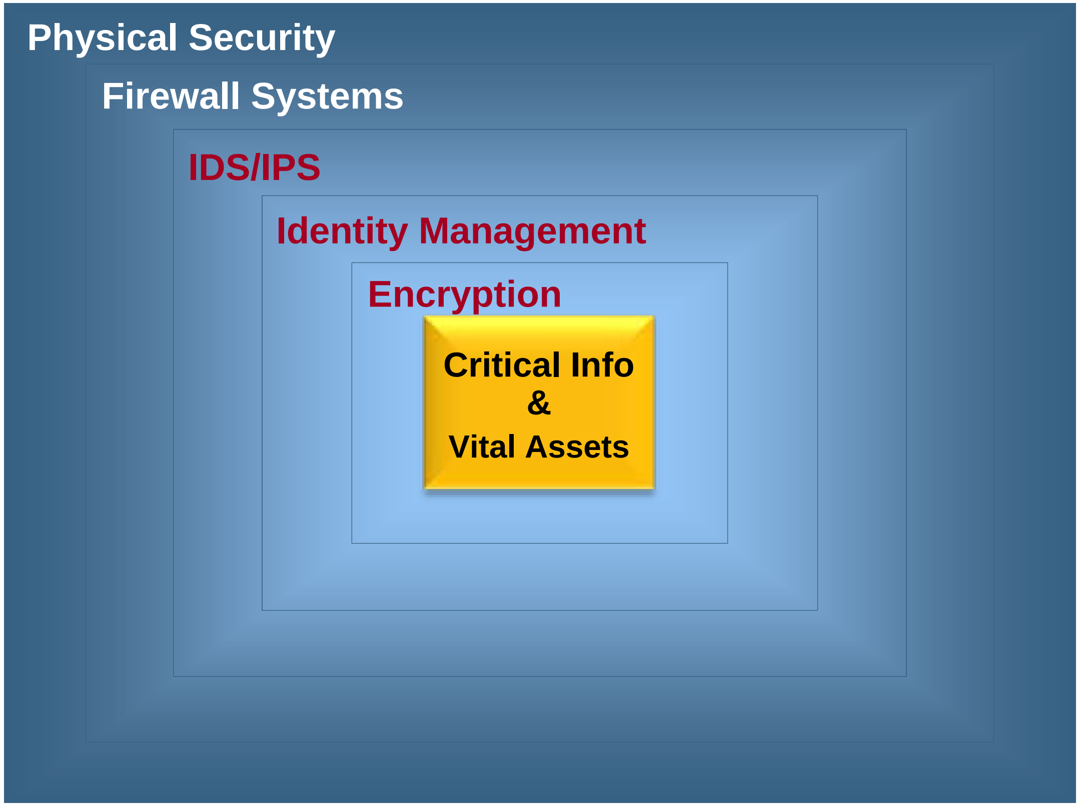
NIST SP 122
PII – A Checklist of What You Must Address

1. Has the organization clearly identified all PII residing in the enterprise?
2. Has the organization categorized PII?
3. Are you applying appropriate safeguards based on confidentiality impact level?
4. Is the collection and retention of PII limited to what is strictly necessary?
5. Have you developed an incident response plan to handle breach of PII?
6. Has the organization established a “forum” to enable close coordination between privacy officers, CIO, security officers and legal?

This checklist must be completed on a regular schedule

Information Security Program Strategy

Core** to the **Edge** and the **Cloud



Security Strategy Must be Risk-based, Pro-active, Integrated!

Checklist for Compliance

Preparing for Audits

- ❑ Entity-wide Security Plan
- ❑ Risk Analysis (last time conducted was?)
  - Technical Vulnerability Assessment (align with Risk Analysis)
- ❑ Risk Management Plan (addressing risks identified in the Risk Analysis) - this is your Corrective Action Plan (CAP)
- ❑ Security violation monitoring reports (incident management)
- ❑ Contingency Plans (last time BIA conducted was?)
- ❑ List of all user accounts with access to systems which store, transmit, or access EPHI (for active and terminated employees)
- ❑ Encryption or equivalent measures implemented on systems that store, transmit, or access EPHI
- ❑ Policies updated, approved and communicated
- ❑ Training for all members of the workforce

Pabrai's Laws of Information Security

Is Your Security Kismet or Karma?

1. There is no such thing as a 100% secure environment
2. Security is only as strong as your weakest link
3. Security defenses must be integrated and include *robust* (passive) and *roving* (active) controls to ensure a *resilient* enterprise
4. Security *incidents* provide the foundation for security *intelligence*

Is Your Enterprise Security?

Kismet **–** A Reactive Security Framework

Karma **–** A Proactive Security Framework

About ecfirst

Compliance & Security

Industry leader delivering world-class services in the areas of compliance and information security for over a decade

Recognized as an Inc. 500 Business in 1st Year of Eligibility

Minority Business Enterprise Certified

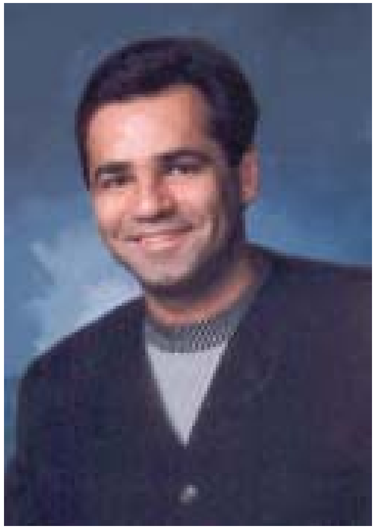
Unique, business-driven, compliance and security solutions; based on the proprietary BizShield™ methodology

***Over 1,600 Clients served including* Microsoft, Cerner, McKesson, HP, PNC Bank and hundreds of hospitals, government agencies**

Contact: John.Schelewitz@ecfirst.com
Phone: +1.480.663.3225

Your Speaker

Control Your Excitement!



Ali Pabrai, **MSEE, CISSP (ISSAP, ISSMP)**

Healthcare Information Security & Compliance Expert

- **Created BizShield™ – *an ecfirst Signature Methodology* - to address compliance and information security priorities**
- **Featured speaker at compliance and security conferences worldwide**
- **Presented at Microsoft, Intuit, E&Y, Federal & State Government agencies & hundreds of other organizations**
- **Consults extensively with healthcare organizations and business associates**
- **Established the HIPAA Academy and CSCS Program– gold standard for HIPAA, HITECH compliance solutions**
- **Member, FBI InfraGard**
- **Follow Pabrai on Twitter, LinkedIn**
- **Pabrai@ecfirst.com**

Download Cyber Security Strategy **Exec Brief PDF @**
www.ecfirst.com – Free to HIPAA Summit Attendees

ecfirst