Information Security Management System: The Compliance Highway to Security Road

IT Governance, Risk Management & Compliance Team

IS&T Children’s Healthcare of Atlanta
Introductions

Diana Candela, CEH, CNDA, ECSA, LPT, NIMS, ITIL, CSSGB
Manager, Information Security GRC

Not-for-profit healthcare system includes:

• 3 Hospitals: one of the largest pediatric systems in the country
• 27 neighborhood locations, including Marcus Autism Center and 6 Urgent Care Centers
• Access to more than 60 pediatric specialties and programs
• More than 900,000 patient visits annually with 350,000 unique patients
• Patients from all 159 counties in Georgia
Agenda

- Security vs Compliance
  - Understanding Security & Compliance
- Selecting a Framework
- ISMS: Governance, Risk & Compliance
- Inclusive Info Sec Management
- Business Value & Benefits
- Owning Risk
- ISMS & IT Service Management
- ISO 27001 Components
- Actions to address Risks & Opportunities
- Implementing an ISMS
- Certification
The struggle IS real!

Compliance ≠ Security

Compliant companies have suffered significant breaches

Security must go beyond compliance requirements

“Checking the Box” is NOT Enough!

Compliance ensures baseline protection

Compliance requirement changes are slow

The Threat Landscape changes fast
Understanding Security & Compliance

Protection of Data = Security + Compliance

**Compliance** involves:

- People, Process, Technology
- “Cookie-cutter” approach
- The “are we” and “how”

**Security** involves:

Understanding **WHY**?

*Always look for opportunities to Integrate Security into your Process*
## Selecting a Framework

### How do different Frameworks deal with emerging risks?

<table>
<thead>
<tr>
<th>Framework</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
</table>
| **ISO 27001** | • Respected internationally  
• Universally understood  
• Comprehensive coverage  
• Policy to operational  
• Technical implementation | • Very subjective  
• Explicit scope of controls  
• Scope too narrow / broad  
• Requires formal attestation |
| **NIST CSF** | • Easy to understand  
• Clearly defined categories  
• Clearly defined control areas  
• Maps to other standards  
• Security program elements | • Very high level  
• More useful in public sector  
• Lots of effort to get tactical  
• No formal accreditation |
| **ISF** | • Specific recommendations  
• Numerous control areas  
• Clearly defined control areas  
• Updated very frequently  
• Includes metrics | • Group relies on consensus  
• Members shape standard  
• Subjective program  
• Not considered neutral |

### Adaptable & Flexible

- **ISO 27001**
- **NIST CSF**
- **ISF**

### Trying to Keep it Simple

- **ISO 27001**
- **NIST CSF**
- **ISF**

### Standard of Good Practice

- **ISO 27001**
- **NIST CSF**
- **ISF**
ISMS: Governance, Risk & Compliance

Information is an asset with value and needs to be appropriately protected

- Protect C.I.A.
- Reduce Risk
- Integrate Security

Leading International Standard for Information Security Management
Inclusive Info Sec Management

- Establish acceptable Policies and security objectives
- Sustain the integration of Info Sec requirements with business process
- Achieve efficiencies with basic process and resources
- Meet diverse organization Info Sec objectives
- Comply with Info Sec Training & Awareness requirements
- Meet Information Security and regulatory compliance objectives
- Endorse and promote Continual Improvement actions
- Establish an Information Security leadership culture
**Business Value & Benefits**

**Information Security Management System**

Management of InfoSec for **all** information systems, people, policies, processes, and technologies.

**Enables Data Breach Protection**

- **Consistent delivery of services**
- **Manage and minimize risk exposure**
- **Protect assets**
- **Keep confidential information secure**
- **Provide secure exchange of information**

Empower staff to contribute to Information Security Management effectiveness with demonstrated commitment across all elements of ISMS.
Owning Risk

Change the conversation!
From: technology solutions
To: managing Risk and Impact

Build alliances!
Achieve clarity on Roles & Responsibilities
Define ownership of Info Sec Risk

Implement programs!
Acceptable Policies & Procedures
Ongoing Risk Mitigation

Accountability!
More productive interaction
Timely risk assessments
ISMS & IT Service Management

Policy
- Standards
- Guidelines
- Procedures

Service Agreement
- Continual Improvement
- Service Operations
- Service Transition
- Service Design
- Operating Level
- SLA

Service Agreement
- Continual Improvement
- Service Operations
- Service Transition
- Service Design
- Operating Level
- SLA
ISO 27001 Components

Establishment and execution of an Information Security Management System (ISMS)

Creation of a Risk Management or Treatment Plan

Creation of “Statement of Applicability” & “Scope and Boundaries”

Creation of a Risk & Compliance Committee or equivalent

An enterprise information security policy

Standard operating procedures (SOPs)
**Actions to address Risks & Opportunities**

*Always* think about / document: Risks & Opportunities

Impact: Focus on “*probable*” vs “*possible*”

Define your organizational “*risk appetite*”

Focus on “*knowable*” risks

Minimize *only the obvious risks*

Information security risks cannot be objectively, rationally and accurately calculated or measured mathematically.
Implementing an ISMS
Certification

Certification means that the organization has an ISMS in place that complies with the ISO 27001 standard.

Certification is obtained from an accredited auditor

Getting certified is NOT required

Certification Doesn’t Equal Security

To achieve Security: Focus on Process, Not Compliance
Questions?

www.choa.org