Information Security Management 101: The Fundamentals

Mapping Key Strengths and Areas of Ownership to Resources
Agenda

- Scenarios
- An ISO Approach
- Key Strengths and Areas of Ownership
- Resources
Scenarios
Where Are You?

• You’re not working in infosec yet, but you desperately want to move into that field.

• You’re a newly minted CISSP with your eyes on a position in infosec management / leadership.

• You’ve recently accepted an infosec management / leadership position in a company that doesn’t have an established (formalized) security program.

• You’ve been in security management / leadership for years, and you want to take a step back and look at the entire program to determine whether or not you’re covering all the bases.

• You’ve recently made a move into consulting, and you want to ensure that your service offerings are appropriate for large enterprises and small / medium businesses.
An ISO Approach
Key Points About ISO 27k

- **International Standard**
  - Actually, sixteen (16) standards
  - 27000 – 27008, 27010 – 27011, 27031, 27033-1, 27044-1, 27035
  - 27799: ISO27k for the healthcare industry

- **27001**: Information technology -- Security techniques -- *Information security management systems -- Requirements*

- **27002**: Information technology -- Security techniques -- *Code of practice for information security management*
  - Twelve (12) categories of security management

- Formal Certification vs. Informal Adoption
  - Your mileage may vary
ISO Security Management Categories

- Risk Management
- Policy Management
- Security Organization Management
- Asset Management
- HR Security Management
- Physical Security Management
- Security Operations Management
- Access Management
- Information Security Systems Management
- Security Incident Management
- Business Continuity Management
- Compliance Management
Today’s Approach

- Ask questions
- Identify controls
- Build your checklist
  - Starting point
  - In the end, it’s about trust and discipline
Plan-Do-Check-Act (PDCA)

Diagram by Karn G. Bulsuk (http://www.bulsuk.com)
Risk Management

• Questions
  ▫ What could go wrong?
  ▫ How do our controls stack up?
  ▫ Are we spending a dollar to protect a dime?
  ▫ What’s our risk appetite?

• Controls
  ▫ Perform a risk assessment
    • Risk = Likelihood x Impact
    • NIST (800-37)
    • FAIR (Factor Analysis of Information Risk)
Policy Management

• Questions
  ▫ What rules do we expect our employees to follow?
  ▫ How do we do what we do?

• Controls
  ▫ Policies, Standards, Procedures
    • Policy = Rules, high level
    • Standard = Technical requirements, detailed
    • Procedure = Step-by-step instructions
  ▫ Starting point = three(3) critical policies
    • Information Security Policy
    • Data Classification Policy
    • Acceptable Use Policy
  ▫ If you expect employees to know what’s expected of them, you have to write it down!
Security Organization Management

• Questions
  ▫ Who’s going to do all this?

• Controls
  ▫ Executive Sponsorship
  ▫ Information Security Steering Committee
  ▫ Information Security Team
    • Internal vs. External (NDA!)
    • Matrixed
Asset Management

• Questions
  ▫ What information assets do we have?
  ▫ How do systems enter the organization?
  ▫ What do we do with retired systems?

• Controls
  ▫ Asset tracking system
    • Discovery
    • Inventory
  ▫ Technology Purchase Request form
HR Security Management

• Questions
  ▫ Do we have job descriptions for the security team?
  ▫ Do our employees really know what’s expected of them?
  ▫ Should we be doing background checks or credit checks on any employees?

• Controls
  ▫ Job Descriptions
    • Manager, Senior Analyst, Analyst
  ▫ Non-Disclosure Agreement (NDA)
  ▫ Security Awareness Training
  ▫ Onboarding and Separations Procedures
Physical Security Management

• Questions
  ▫ What’s our perimeter?
  ▫ Could someone walk into any of our locations and take something that doesn’t belong to them?

• Controls
  ▫ Locks
    • Sensitive areas
  ▫ Badges
    • Employee, Contractor, or Visitor?
  ▫ Physical Security Assessment
Security Operations Management

• Questions
  ▫ Who’s responsible for the day-to-day security stuff?
  ▫ What exactly is the day-to-day security stuff?

• Controls
  ▫ Security Operations Procedures
    • Change Control
  ▫ Antimalware
  ▫ Encryption
  ▫ Logging and Monitoring
    • Enabled, centralized, and detailed
Access Management

• Questions
  ▫ Does everyone have access to what they need in order to do their jobs?
  ▫ Can unmanaged devices attach to our network?

• Controls
  ▫ Principle of least privilege
  ▫ Centralized user directory
  ▫ Access reviews
  ▫ Password management
  ▫ Lock screens
  ▫ Multi-factor authentication
  ▫ Port security
Information Security Systems Management

• Questions
  ▫ How do we secure new systems before we add them to our network?
  ▫ Do we have production data in non-production systems?

• Controls
  ▫ System hardening process
  ▫ Software Development Lifecycle (SDLC)
  ▫ Change control procedures
    • Change Approval Board (CAB)
  ▫ Vulnerability management procedures
    • Development, QA, Production
    • Scan EVERYTHING (hosts, databases, apps)
    • Penetration testing (validate your controls)
Security Incident Management

• Questions
  ▫ What could go wrong?
  ▫ What’s already gone wrong?
  ▫ What do we do when something goes wrong?

• Controls
  ▫ Security Incident Response
    • One Policy
    • Many Procedures
  ▫ Security Information Event Management (SIEM) system
  ▫ Training
    • End User Security Awareness
    • Incident Response
    • Forensics
  ▫ Tabletop Exercises
Business Continuity Management

• Questions
  ▫ How will we recover from a disaster?
  ▫ How will we keep the business going during the recovery process?

• Controls
  ▫ Disaster Recovery Plan
  ▫ Business Continuity Plan
  ▫ Backups
  ▫ Tabletop Exercises
Compliance Management

• Questions
  ▫ What do I need to comply with?
    • HIPAA, PCI, NERC/FERC, SOX, COPPA, etc.
    • External and Internal

• Controls
  ▫ Documented Compliance Procedures
    • Who is responsible for what?
    • When is it due?
  ▫ Unified Compliance Framework
  ▫ Audits
    • External and Internal
    • Scheduled, non-intrusive, and independent
Key Strengths and Areas of Ownership
Skillset Groupings

<table>
<thead>
<tr>
<th>Business (People)</th>
<th>Process</th>
<th>Technical (*ology)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Organization</td>
<td>Risk</td>
<td>Physical</td>
</tr>
<tr>
<td>HR Security</td>
<td></td>
<td>Asset</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>Security Operations</td>
<td></td>
</tr>
<tr>
<td>Security Incident</td>
<td>Information Security Systems</td>
<td></td>
</tr>
<tr>
<td>Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This chart identifies key strengths, which align with areas of ownership.
Business Skillset

- “People person”
- Information security governance
- Compliance and regulatory knowledge
- Understand integration points among business, security, and compliance
- Managing people
- (ISC)2 CISSP and/or ISACA CISM
  - Hardcore = SANS Masters Degree in Information Security
Process Skillset

- Accountant
- Blend of business and technology
- Policies, standards, procedures
- Understanding of business process flows
- ISACA CISA
Technical Skillset

- Geek / Nerd
- System administration
- Active in technical/security user groups
- Deep knowledge of specific technologies
- (ISC)² CISSP + Specific tech certs
Core Team

- **Manager**
  - Business-oriented, with understanding of tech and process
  - The buck stops here
  - Strategic

- **Senior**
  - Highly Technical and Process-Oriented, with business knowledge
  - Primary and Secondary
  - Strategic + Tactical

- **Junior**
  - Technical and Process-Oriented
  - Primary and Secondary
  - Tactical + Operational
Sample Org Chart

Manager
-> Security Organization

Technical (Senior)
-> Security Operations
-> Information Security Systems

Technical (Junior)
-> Security Operations
-> Physical
-> Asset

Process (Senior)
-> Policy
-> Risk
-> Business Continuity
-> Security Incident

Process (Junior)
-> Policy
-> HR
-> Compliance
-> Security Incident
Resources
Resources

• Wikipedia

• International Organization for Standardization
  ▫ ISO/IEC 27001:2005
    • http://www.iso.org/iso/catalogue_detail?csnumber=42103
  ▫ ISO/IEC 27002:2005
    • http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

• The ISO 27000 Directory
  ▫ http://www.27000.org/iso-27001.htm

• ISO 27001 Security <- GREAT starting point
  ▫ http://www.iso27001security.com/
More Resources

• Other Frameworks
  ▫ COBIT (IT Governance)
    • http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
  ▫ ITIL (IT Service Management)
    • http://www.itil-officialsite.com/
  ▫ Unified Compliance
    • https://www.unifiedcompliance.com/

• Risk Management
  ▫ NIST
  ▫ FAIR
    • http://www.cxoware.com/
    • http://fairwiki.riskmanagementinsight.com/
Even More Resources

- SANS 20 Critical Security Controls

- GIAC Certified ISO-27000 Specialist
  - [http://www.giac.org/certification/certified-iso-27000-specialist-g2700](http://www.giac.org/certification/certified-iso-27000-specialist-g2700)

- Australian Department of Defence Top 35 Mitigation Strategies

- Information Security... Simplified
  - [http://www.infosecsimplified.com/](http://www.infosecsimplified.com/)

- IT Security Career
Professional Organizations

• ISSA (Information Systems Security Organization)
  ▫ http://www.issa.org/

• ISACA (Information Systems Audit and Control Association)
  ▫ https://www.isaca.org/

• SANS
  ▫ http://www.sans.org/

• InfraGard
  ▫ http://www.infragard.net/

• OWASP (Open Web Application Security Project)
  ▫ https://www.owasp.org/
Questions / Contact Info

Jerod Brennen, CISSP
http://www.linkedin.com/in/slandail
http://twitter.com/#!/slandail

http://www.jacadis.com/
contact@jacadis.com