Preparing for a Compliance Audit
Knowing the answers to the questions

Presented by:
Bill Curtis
SynerComm, Inc.
bill.curtis@synercomm.com
www.synercomm.com
Compliance Audit Readiness

• Compliance audits are necessary but do not need to be painful.

• Being prepared for an audit is so much more than the ability to show an auditor what they need to see. Being prepared for an audit is when an organization already knows the answers to the questions.

• You cannot manage what you do not understand.

• Compliance readiness is:
  • The ongoing alignment of your business to a baseline standard(s)
  • Aligning IT, System and Data Owners (SDO), and leadership
  • Assessing readiness (compliance) to selected standard(s)
  • Remediating gaps, POAM
  • Developing a business-as-usual atmosphere

• This session will explore best practices to develop and execute an effective information systems compliance program.

Tweet along: #Sec360

www.Secure360.org
You Cannot Manage What You Do Not Understand

- Data
- Systems
- Processes
- Owners
- Compliance requirements

Tweet along: #Sec360

www.Secure360.org
Compliance Readiness

• Get your house in order
  • Select a Framework(s)
  • IT and Business Alignment

• Determine your current state
  • Assess Against a Framework(s)

• Improve your current state
  • Close Framework Gaps

• Maintain
  • Institute Steady State ‘Business-as-Usual’ Activities

Tweet along: #Sec360
www.Secure360.org
Compliance Readiness
Control Frameworks
Compliance Readiness
Control Frameworks

Framework definition:

An essential supporting structure of a building, vehicle, or object.

A basic structure underlying a system, concept, or text.

Information System Framework Examples:

• NIST – National Institute of Standards and Technology
• PCI – Payment Card Industry
• HIPAA – Health Insurance Portability and Accountability Act
• CSA – Cloud Security Alliance
• CIS – Center for Internet Security
Compliance Readiness Controls Framework

NIST SP800-53 Revision 4
Compliance Readiness
Controls Framework


• NIST states:
  • Special Publication 800-53, Revision 4, provides a more holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate—contributing to systems that are more resilient in the face of cyber attacks and other threats.
# Compliance Readiness

**NIST SP800-53 Rev4**

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC: Access Control</td>
<td>MA: Maintenance</td>
</tr>
<tr>
<td>AP: Authority and Purpose (*)</td>
<td>MP: Media Protection</td>
</tr>
<tr>
<td>AR: Accountability, Audit, and Risk Management (*)</td>
<td>PE: Physical and Environmental Protection</td>
</tr>
<tr>
<td>AT: Awareness and Training</td>
<td>PL: Planning</td>
</tr>
<tr>
<td>AU: Audit and Accountability</td>
<td>PM: Program Management Controls (*)</td>
</tr>
<tr>
<td>CA: Security Assessment and Authorization</td>
<td>PS: Personnel Security</td>
</tr>
<tr>
<td>CM: Configuration Management</td>
<td>RA: Risk Assessment</td>
</tr>
<tr>
<td>CP: Contingency Planning</td>
<td>SA: System and Services Acquisition</td>
</tr>
<tr>
<td>DI: Data Quality and Integrity (*)</td>
<td>SC: System and Communications Protection</td>
</tr>
<tr>
<td>DM: Data Minimization and Retention (*)</td>
<td>SE: Security (*)</td>
</tr>
<tr>
<td>IA: Identity and Authentication</td>
<td>SI: System and Information Integrity</td>
</tr>
<tr>
<td>IP: Individual Participation and Redress (*)</td>
<td>TR: Transparency (*)</td>
</tr>
<tr>
<td>IR: Incident Response</td>
<td>UL: Use Limitation (*)</td>
</tr>
</tbody>
</table>

Tweet along: #Sec360

www.Secure360.org
Compliance Readiness
Controls Framework

CIS Top 20 Critical Security Controls, V6.1
Compliance Readiness
Control Frameworks

• [http://www.cisecurity.org](http://www.cisecurity.org)

• CIS states:
  • “Fog of More: competing options, priorities, opinions, and claims that can paralyze or
distract an enterprise from vital action.”
    • Technology, Information, Oversight
      • Security tools
      • Security standards
      • Training and classes
      • Certifications
      • Vulnerability databases
      • Guidance, benchmarks, recommendations and best practices
      • Catalogs of security controls and countless security checklists

• These are the kinds of issues that led to and now drive the CIS Critical Security
Controls. They started as a grass-roots activity to cut through the “Fog of More”
and focus on the most fundamental and valuable actions that every enterprise
should take.
## CIS Top 20 Critical Security Controls, V6.1

<table>
<thead>
<tr>
<th>CSC 1: Inventory of Authorized and Unauthorized Devices</th>
<th>CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC 2: Inventory of Authorized and Unauthorized Software</td>
<td>CSC 12: Boundary Defense</td>
</tr>
<tr>
<td>CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers</td>
<td>CSC 13: Data Protection</td>
</tr>
<tr>
<td>CSC 4: Continuous Vulnerability Assessment and Remediation</td>
<td>CSC 14: Controlled Access Based on the Need to Know</td>
</tr>
<tr>
<td>CSC 5: Controlled Use of Administrative Privileges</td>
<td>CSC 15: Wireless Access Control</td>
</tr>
<tr>
<td>CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs</td>
<td>CSC 16: Account Monitoring and Control</td>
</tr>
<tr>
<td>CSC 7: Email and Web Browser Protections</td>
<td>CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps</td>
</tr>
<tr>
<td>CSC 8: Malware Defenses</td>
<td>CSC 18: Application Software Security</td>
</tr>
<tr>
<td>CSC 9: Limitation and Control of Network Ports, Protocols, and Services</td>
<td>CSC 19: Incident Response and Management</td>
</tr>
<tr>
<td>CSC 10: Data Recovery Capability</td>
<td>CSC 20: Penetration Tests and Red Team Exercises</td>
</tr>
</tbody>
</table>
Compliance Readiness
Control Frameworks

- Framework Orientation:
  - Bring IT and the business along
  - C-level suite endorsement
  - Alignment to a compliance initiative
  - Create a Controls Culture
- Training 101:
  - You can not manage what you do not understand.
  - Control workshop:
    - Explain control intent
    - Discuss and guide adoption
    - Schedule recurring meeting to work through the control families
  - Map out the process:
    - Achieve compliance
    - Maintain compliance (business-as-usual)
Compliance Readiness
IT and Business Alignment

• In a business environment where resources are limited, compliance requirements abound, and budgets are constantly challenged to meet cost containment targets an organization must:
  • Align IT and IS, system and data owner(s), and leadership.
    • Objective: awareness, engagement, buy-in (support)
    • All hands on deck
  • Raise awareness and appreciation of your organization’s information systems’ value, exposures (risk), and operating plan (controls).
  • Develop an effective information systems compliance program.
    • Plan, Do, Check, Act
  • Adopt a business as usual approach.

Tweet along: #Sec360 www.Secure360.org
Compliance Readiness
IT and Business Alignment

• First, a few definitions / players: (may seem obvious, but let’s be sure)
  • Information Technology and Information Security (IT/IS): The stewards or custodians of systems and data. Responsible for ALL facets of care and feeding.
    • ** IT and IS
      • One is not necessarily inclusive of the other
      • Responsibility for CIA
  • System and Data Owners (SDO): Those within the business who own business systems, applications and/or data.
    • Formally or informally assigned
    • More than one (likely multiple)
    • Responsibility for CIA
  • Leadership (L):
    • Senior management and business unit owners:
      • Business planning and financial targets, communicates plan (anticipated performance) to interested parties (shareholders, stakeholders, a committee or board) and drives the business for results.
      • Responsibility for CIA

Tweet along: #Sec360
www.Secure360.org
Compliance Readiness
IT and Business Alignment

• Problem Statement: Within many organizations’ shortcomings exist in the establishment of:
  • Clear understanding (outside of IT) of composition of information systems:
    • Complexity, capability and limitations, threats and vulnerabilities
    • Compliance requirements
  • Clear understanding of what matters most to System and Data Owners (SDO)
  • Relationship between players; IT/IS, SDO, Leadership
  • Business processes that:
    • Raise awareness of the ‘Total Information Systems Picture’
    • Identify, evaluate and address system and data risk
    • Engages IT/IS, SDO and Leadership in ‘information systems decisions’
    • Become business as usual
Compliance Readiness
IT and Business Alignment

- Information Systems Decisions (aka – effective communications):
  - Addition of a new system, application or data
  - Decisions / changes impacting a system, application or data
  - Decisions / changes impacting controls effectiveness
  - Risk mitigation strategy and/or acceptance
  - Business continuity and incident response planning
  - IT/IS budget ‘negotiations’
  - Staff additions / changes
  - Service level agreements definition / performance

Tweet along: #Sec360
Compliance Readiness
IT and Business Alignment

• Recipe for Effective Communications:
  • Assignment of system and data ownership
  • Getting the right folks together:
    • Committee / governance
    • Risk and performance assessments
    • Change review board (with power to cancel a change)
      • 100% of changes // 100% of the organization // 100% of the time
  • Establishing common ground / language (framework):
    • Adoption of framework and integration of its terms and language
      • Business as usual
  • SWOT Analysis - ongoing dialog:
    • Strengths
    • Weaknesses
    • Opportunities
    • Threats

Tweet along: #Sec360
www.Secure360.org
Compliance Readiness Assessment
Compliance Readiness
Assess Against a Framework

• Assess the intent of a control against the reality of the system
  • It will take time
  • Whomever is assessing MUST understand the controls framework.
  • There will be gaps and unanswered questions:
    • POAM
  • Assemble audit artifacts:
    • System Security Plan
    • Policies and standards
    • Configuration guidelines
    • Screen shots
    • Reports
Compliance Readiness
Assess Organization Readiness

• Review existing policies and procedures (if they exist)
• Interview management, IT, risk/compliance, and business unit employees to identify organization characteristics such as:
  • Accountability (top down and bottom up)
  • Business model (who are we, what do we do, how do we do it)
  • Data considerations and regulations (electronic and hard copy)
  • Risk, compliance, and audit function
  • Vendor and customer management
  • SDO function
  • Information technology function
  • Information security function

Tweet along: #Sec360
www.Secure360.org
Compliance Readiness
Risk Assessment

• Discover Assets (what do we have and how do we rank its risk level)
  • Core business processes
  • Systems and data inventory
    • Ranking criteria

• Assess System and Data Risk (what could [will] go wrong and what are we doing to offset the potential impact)
  • Threats and vulnerabilities
  • Controls
    • Controls effectiveness review and action plan to close gaps
      • Measure of controls effectiveness
        • Policies and standards
        • Interview and testing of technical controls
Compliance Readiness
Improve Your Current State
Compliance Readiness
Improve Your Current State

• Assemble assessment results and rank risk
  • Organization assessment
  • Technical (systems and data) assessment

• Strengthen your organization’s:
  • Information Security Management System (ISMS)
  • System Security Plan (SSP)
  • Readiness

• Continually assess and improve
  • Leverage the Plan of Actions and Milestones (POAM) approach

• Leverage an IT Governance Framework
Compliance Readiness
Maintain
Compliance Readiness
Maintain

• Create a culture of business-as-usual
  • Engaged IT/IS, SDO and leadership
  • Alignment to controls framework(s)
  • ISMS
    • Maintained and easily accessible
• Monitor risk profile:
  • Assets, threats and vulnerabilities, controls
• Ensure failures in security controls are detected and responded to
  • Monitoring, reporting and response
• Review changes to the environment (100%)
• Assess changes to the organization
• Perform periodic reviews (spot-checks)
• Stay current with hardware and software technologies

Tweet along: #Sec360
www.Secure360.org
Questions?
Thank You

Tweet along: #Sec360

www.Secure360.org