



Regulatory Compliance

How to get – and stay – compliant...

NW CIPS Summit

August 4th, 2006

Lake Oswego, OR

Patrick Miller CISSP-ISSAP, CISA

The Current Situation

- Corporate Accountability and Fraud
 - Enron, WorldCom, etc...
 - Id Fraud, Data Breaches, etc...
- Economic Challenges
 - Ripple effect from war(s), oil prices, interest rates, etc; costs are increasing
 - Mandates to do more work with less; budgets are only getting tighter
- Technology Shift
 - Automation is everywhere, doing more work with fewer people
 - Technology gets cheaper by the day, human expertise doesn't
 - Ever-increasing complexity, power and integration/interconnectivity
- Terrorism and Cyber-crime
 - Can they use our people, processes, or technology against us?
 - Organized crime discovered they could hack for profit
- Lack of Expertise and Experience
 - New talent is scarce; old talent is rapidly exiting the company
 - Security "snake oil" is common; no "easy button"

We Are Not Alone...

- 
- Sarbanes-Oxley
 - HIPAA
 - GLBA
 - CJIS
 - PCI
 - California SB1386
 - CIP-002 through 009
 - AGA-12
 - MTSA (ISPS)
 - SAFETY Act
 - FIPS/FISMA

Just to name a few...

Regulatory Landscape

Why all the new regulations?

- Aside from the current situation...
- Aside from PDD 67 and HSPD 7...
- Most organizations are **not** implementing good security
- Most organizations do **not** disclose when/how they were hacked (if they know)
- Disagreement on what "good security" actually is or should be
- Unclear or lack of visibility into security within organizations
- Technology has altered the risks; good timing
- Industry self-regulation is getting bad press for moving too slow

When will it get better?


- Resolve competing security standards that overlap or even conflict
- Many Federal agencies producing these regulations fail their own audits!
- Yes, but it will be a while, so put on your seatbelt and hang on for the ride...

Common Threads

They all have very similar roots...

- Driven by PDD 67 and HSPD 7
- Built on-or-from ISO 17799/27001
- Risk-based assessments are always Step #1
- Definitely not perfect in current implementations, but the advice is still sound
- None of this is new – based on time-tested general security principles that work for both physical and information assets

General Security Principles

- 
- Defense in depth
 - Least privilege; need to know
 - Separation of duties
 - Keep it simple; complexity increases risk
 - Keep it separate
 - Create distinct zones or segments
 - Firewall example - physical/cyber
 - Be practical
 - Don't over-secure (you don't have to outrun the bear)
 - Remember the 80/20 rule; security is an asymptotic curve

Secret Solution

What is the secret to perpetual compliance?

Built-In Security!

- Be proactive, not reactive...
- Don't wait for regulations to begin securing your organization or you will always be catching up
- Security must be built into business processes
- Requisite culture-shift (toward security and auditability)
- Build a framework for compliance to **any regulation**


The Real Story...

Compliance isn't easy...

- Get organized
- Get ownership
- Get educated
- Get help
- Understanding risk
- Managing expectations
- Sustaining compliance



Get Ownership

- 
- Start with the "tone at the top"
 - Letter of the law, or spirit of the law?
 - Establish upstream awareness and acknowledgement at every level to provide appropriate assurance
 - Establish necessary maintenance requirements (maintaining/sustaining compliance is the hardest part)
 - Regular audits to ensure that compliance activities are fully "operationalized."

Get Organized

- Identify Stakeholders and have them provide a team of Subject Matter Experts (SMEs)
- Create standard document templates for everything; maintain consistency in the formatting/presentation of the data
- Document your compliance program approach; even something as simple as a project plan will work
- Identify your criticality criteria and risk-assessment method
- Schedule regular self-assessment and self-audits; report all findings to Stakeholders
- Dashboards and stoplights are a great ideas, and can offer a daily view into the "compliance posture" (works better with good automation); some vendor tools are available

Get Educated

- Read other standards from other industries; remember the Energy Industry is not alone
- Review any/all applicable Risk Assessment Methods
- Review the history of your particular regulation/standard to obtain a better idea of where it is going in the future
- Seek to understand how you will be held accountable; become comfortable with the audit process
- Get involved with industry Working Groups and discuss how peers are evaluating and mitigating their risks
- Pass it on; communicate everything you have learned with your compliance team and peers

Get Help



- More involvement from all areas of the business means less burden on any one particular group
- If the entire business is involved, it will usually take less time and achieve a greater breadth of coverage
- Leverage your IT department expertise with auditable processes; IT already knows how to live within the confines of SOX, CobiT, COSO, ITIL, Visible-Ops, etc...
- Leverage your project management office
- Piggyback on successful operational functions and programs such as Safety

Understanding Risk

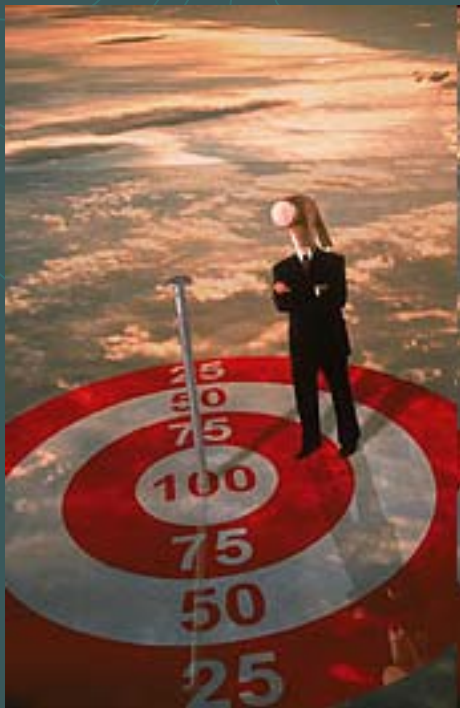
- Risk = Impact/Consequence x Probability/Likelihood – it's a very simple equation. *Keep it that way.*
- Overanalyzing risk can waste time and money; often the qualitative complex risk assessment methods obtain the same result as qualitative simple methods
- Read and evaluate many different risk methodologies
- Don't assume risk on your own. Make it a business decision based on good solid facts (gut instinct can't be avoided). *Remember: Management owns the risk.*
- Understand controls, threats, vulnerabilities, exploits, opportunity and how they relate to risk
- The more you know about risk *and* risk assessment the better you will be able to articulate your position to an auditor



Risk Assessment Resources

- There is no silver-bullet or easy-button tool, and there won't be – *despite what Vendors say*
- In NERC's own words, there are three important questions:
 - What is critical?
 - What is vulnerable?
 - What can be done to reduce the vulnerabilities?
- NERC RAWG Whitepaper
 - <http://www.esisac.com/library-assessments.htm>
- ESISAC – Vulnerability and Risk Assessment
 - <http://www.esisac.com/publicdocs/Guides/V1-VulnerabilityAssessment.pdf>
- NIST 800 series
 - <http://www.csrc.nist.gov/publications/nistpubs/>
- ASIS Guideline
 - <http://www.asisonline.org/guidelines/guidelinesgsra.pdf>
- OCTAVE
 - <http://www.cert.org/octave/>
- Sandia Labs Risk Assessment Classification Scheme
 - http://www.sandia.gov/iorta/docs/SAND2004_4233.pdf
- GAO – Risk Assessment Practices of Leading Organizations
 - <http://www.gao.gov/special.pubs/ai00033.pdf>

Managing Expectations



- Compliance will require a culture-shift; don't try to change too much at once
- Start with a gap analysis to understand just how much work is in front of your compliance team; consider using Maturity Metrics (ISO21827)
- Be as clear as possible as to what is necessary to be done, in terms of labor, budget and time
- Regular, **unvarnished** upstream reporting is vital; keep the chain of command informed of everything related to the compliance effort
- Don't rely on FUD (Fear, Uncertainty and Doubt); keep it real, and keep politics out of the discussion
- It may require an occasional reminder that "doing the right thing" is in the organization's best interest

Sustaining Compliance

- Compliance evidence does not need to be complex. Matter of fact, the simpler the better.
- Have the SMEs or the operational staff develop the processes, procedures and other required documentation for a higher degree of ownership and acceptance
- Get it “operationalized” early and hold people accountable with applicable reporting metrics
- Leverage technology to help meet archival and update requirements
- Automate, automate, automate; avoid manual processes whenever possible; include logical checks to ensure automation is functioning as expected
- Audit yourself regularly; use appropriate internal *and* external resources

Program Elements That Work

- Program architecture spans entire organization
 - Senior Management sponsor – signing official, directs program, accepts risks
 - Stakeholders – managers [and above] with skin in the game
 - Subject Matter Experts – where the rubber hits the road
- Document all known gaps, even the bad stuff; assign [realistic] owners and dates to all issues and hold them to it – drive it like a project
- Capture all decisions, discussions and meetings for the record
- Compliance summary for management; stoplight or dashboard
- Formal process for exceptions/deviations; include risk language
- Strong chain of accountability; require upstream signatures
- Use of logs, audit trails, and any other technical means to establish all necessary evidence; less reliance on human processes where appropriate
- Storage of all documentation and evidence in a tightly controlled central repository; “evidence catalog”
- Regular self-assessment/self-audit checklists

What About the Money?

- Do you spend more on coffee than security?
- Many PUCs/PSCs have openly stated you'll get the money needed to be secure (and compliant)
- Good protection isn't cheap, so spend wisely
- In-house vs. out-sourcing – depends on size
- Don't forget about cost-avoidance; is it cheaper than fines, auditors and lawyers?
- Consider the automobile safety push in the 1970s – Volvo and Subaru capitalized on it
- Be the most reliable company on the block – it's all we've got!

Surviving an Audit

- Sound and comprehensive risk assessment as your baseline; regularly repeat the assessment using the same criteria for consistency
- Strict adherence to your [self-defined] policy, processes and procedures
- Document everything; meeting minutes, decisions, discussions, exceptions...
- Centralized location and format for all compliance documentation
- Certification and signatures all the way upstream, starting with the SME-level
- Only keep/provide what is required as evidence for compliance; don't over-provide – this will minimize drill-down and diversions
- Be smart and confident in your compliance efforts, only you know what is best for your organization; respectfully challenge the auditor if necessary
- Embrace ambiguity in your responses to auditors
 - Only tell them exactly what they need to know, with only as much detail as necessary
 - Do not volunteer anything beyond what is explicitly asked
- Letter vs. spirit of the law
 - Due diligence; due care
 - Don't rely on an auditor's interpretation; compliance should be immediately evident
- No whining; take your licks like a pro (should you get any)

Closing Thoughts...

- You are part of the Critical Infrastructure – **act accordingly and responsibly**
- Whether it's corporate accountability or infrastructure security, the laws are changing and you will be forced to change in response
- Build security and accountability into your everyday processes and compliance will follow
- Build a compliance program to meet anything that may come your way, because it will
- *The auditors and lawyers are coming...*

Questions?

Patrick C. Miller

CISA CISSP-ISSAP SSCP NSA-IAM

Sr. Security Consultant

PacifiCorp Corporate Security

patrick.miller@pacificorp.com

503.813.7014