



# Evidencing Compliance

Patrick Miller – *CISSP, CISA*  
Stacy Bresler – *CISSP, CISA*  
*Corporate Security*  
*March 13<sup>th</sup>, 2006*

# Overview



- Review the First Steps
- Understanding Risk
- Managing Maintenance
- Managing Expectations
- Making an Audit Relatively Painless
- What Works For Us (at least thus far)

## The 4 Gets

---



- Get Organized
- Get Top Management Buy-in
- Get Educated
- Get Help

## Get Organized (step 1)

---

- Who will be leading/organizing the overall effort? Consider a single person for this task...
- Communicate with all relevant Stakeholders of your organization and have them provide a team of Subject Matter Experts (SMEs); assign responsibility for compliance to the SMEs
- Create a standard document template, and use it for everything; maintain consistency in the formatting/presentation of the data
- Centralize, but protect; put all evidence in one location for ease of protection as well as ease of review by an auditor
- Dashboards and Stoplights are a great ideas, and can offer a daily view into the "compliance posture" (works better with good automation)
- Document your compliance program approach; even something as simple as a project plan will work
- Consider Self-Assessment Checklists for the SMEs

## Get Top Management Buy-In (step 2)

---

- Start with the "tone at the top"; if Senior Management doesn't care, you won't get far
- How you go about evidencing is directly related to how your organization decides to address the standard. Are you going to comply to the “letter of the law” or to the “intent of the law?”
- Do not underestimate the on-going maintenance needs of the standard; maintaining and sustaining compliance is the hard part...
- Evidencing is easier if the activity is common and actually “in operations.”
- Regular testing may be required for some time to ensure that compliance activities are fully “operationalized.”

## Get Educated (step 3)

---

- Read other standards from other industries; the Energy Industry is not alone (SOX, AGA-12, GLBA, HIPAA, CJIS, etc)...
- Review the history of your particular regulation/standard to obtain a better idea of where it is going in the future
- Get involved with industry Working Groups and discuss how peers are evaluating and mitigating their risks
- “Know thy enemy” – understand the regulatory entity and how they will be holding you accountable; become comfortable with their process
- Pass it on; communicate everything you have learned with your compliance team

## Get Help (step 4)

---

- The more involvement from all areas of the business, the less burden on any one particular group
- If the entire business is involved, it will usually take less time and achieve a greater degree of consistency overall
- Leverage your IT department expertise to meet your business needs. Especially around “securing location” type requirements...
- Do not try to do this in a silo – use your project management office if you have one
- Take a look at your SOX program [if applicable] – that program probably has a good model to follow
- Piggyback on successful operational functions such as Safety

## Understanding Risk

- Risk = Impact x Likelihood – a very simple equation. Keep it that way.
- Overanalyzing risk can waste time and money; often the qualitative and complex risk assessment methods obtain exactly the same result as a qualitative simple method
- Read and evaluate many different risk definitions and discussions (from qualified authors)
- 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 threats, vulnerabilities, exploits and how they relate to risk; note that they are different, but related...
- The more you know about risk *and* risk assessment the better you will be able to articulate your position to an auditor



©2006 PACIFICORP | PAGE 8

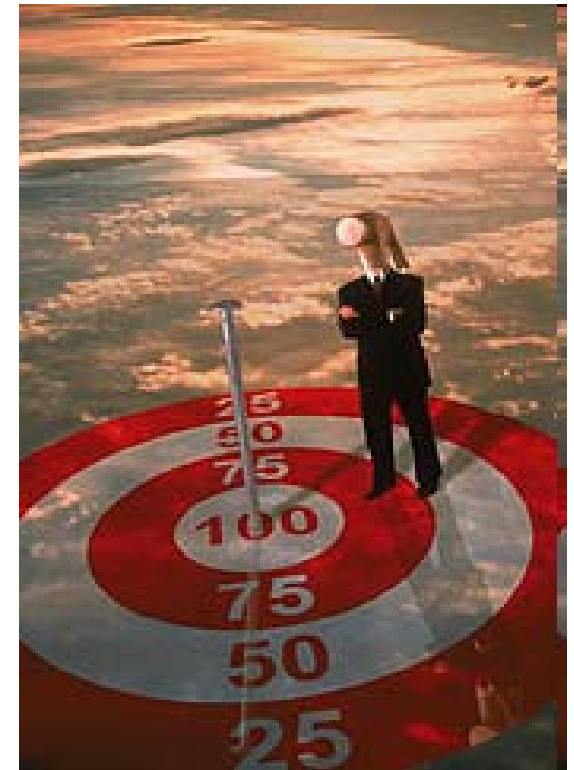
## Managing Maintenance

---

- 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

# Managing Expectations

- Start with a gap analysis to understand just how much work is in front of your compliance team; consider Maturity metrics (ISO21827)
- Be as clear as possible as to what is necessary to be done, in terms of labor, budget and time. Even auditors won't know for sure!
- 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
- Embrace ambiguity. This is your key to success (remember document everything and get levels of understanding/agreement – for example, keep all meeting minutes)
- It may require an occasional reminder that “doing the right thing” is in the organization's best interest



## Making an Audit Relatively Painless

---

- 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
- Centralized location and format for all compliance documentation
- Only keep/provide what is required as evidence for compliance; don't over-provide – this will minimize drill-down and diversions
- Certification and signatures all the way upstream, starting with the SME-level
- Be smart and confident in your compliance efforts, only you know what is best for your organization
- No whining; take your licks like a pro (should you get any)

## What Works For Us (Thus Far)

- Enterprise “project” architecture, even though it is really a “program”
- Senior Management sponsor, Stakeholders, and Workstream Leads (SMEs)
- Self-Assessment Checklists
- Compliance Program Approach
- Compliance Summary w/ Stoplight
- Documentation of all decisions, discussions and meetings; formal process for exceptions/deviations
- 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

