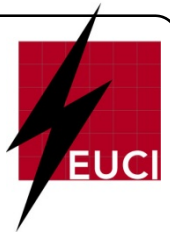




Western Electricity Coordinating Council



CIP Compliance Program Success

EUCI's NERC Standards Conference
Hyatt Regency, Irvine, CA
February 25th, 2009

Patrick Miller CISA CISSP-ISSAP
WECC Sr. Compliance Engineer, Cyber Security

Overview

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



Get Ownership

- “Tone at the top“ (Executive Ownership)
- Accountability (Management Ownership)
 - Establish upstream awareness and acknowledgement at every level to provide appropriate assurance
- Auditability (Oversight Ownership)
 - Regular audits (internal and external) to validate compliance posture
- Sustainability (Operational Ownership)
 - Establish maintenance requirements - sustaining compliance is the hardest part

Get Organized

- Ramp up
 - End-to-end plan; document your compliance program approach
 - Allocate funding and resources (Stakeholder and SME owners)
 - Start executing the plan in small steps
- Assess
 - Schedule regular self-assessment and self-audits
 - Report all findings to Stakeholders as early as possible
- Stay Informed
 - Keep everyone at all levels informed of compliance status
 - Dashboards, etc (automation helps; some vendor tools are emerging)
- Standardize Documentation
 - Consistency in the formatting/presentation of the data is beneficial

Get Educated

- Start with a history lesson...
- Leverage existing compliance experience
 - SOC (888/889/890), Sarbanes-Oxley, EPA, CFATS, etc
- Understand “risk”
- Understand “outside influences”
- Get to know Regulatory strata
- Events, Working Groups, User Groups, Task Forces, etc – networking is essential

Get Help

- Share the load
 - Greater 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 existing expertise with auditable processes
 - IT already knows how to live within the confines of SOX, CobiT, COSO, ITIL, ITSM, ISO 27005*
- Involve project management and internal audit
- Piggyback on successful operational functions and programs such as Safety, Training, etc

Understand Risk

- In most cases Risk = Impact x Probability
 - **Not in this case...**
- Risk is now just Impact/Consequence
 - Set Probability to 100% (or in other words, ignore it)
- Good guidelines
 - NERC Guidelines
 - WECC RBAM (coming soon)
 - OCTAVE Allegro
- Don't overanalyze; qualitative vs. quantitative
- Don't assume risk on your own
 - Ask all of the right people all of the right questions
 - Base risk decisions on good solid facts, studies

Manage Expectations

- Compliance will require a culture-shift
 - Don't try to change too much at once
- Start with a gap analysis
 - Get a real picture of the work ahead
 - Consider using Maturity Metrics such as ISO21827, CobiT, etc
- Regular, unvarnished upstream reporting is vital
- Don't rely on FUD (Fear, Uncertainty and Doubt)
 - Honesty and reality is the best approach

Sustaining Compliance...

- Keep policies, processes and evidence simple
- Have the SMEs or the operational staff develop the processes and procedures
- Get it “operationalized” early
 - Establish accountability with applicable reporting metrics
- Automate
 - Avoid manual processes whenever possible
 - Include logical checks to ensure automation is functioning
- Get compliance items into your RFPs and contracts
 - SCADA Procurement Language project

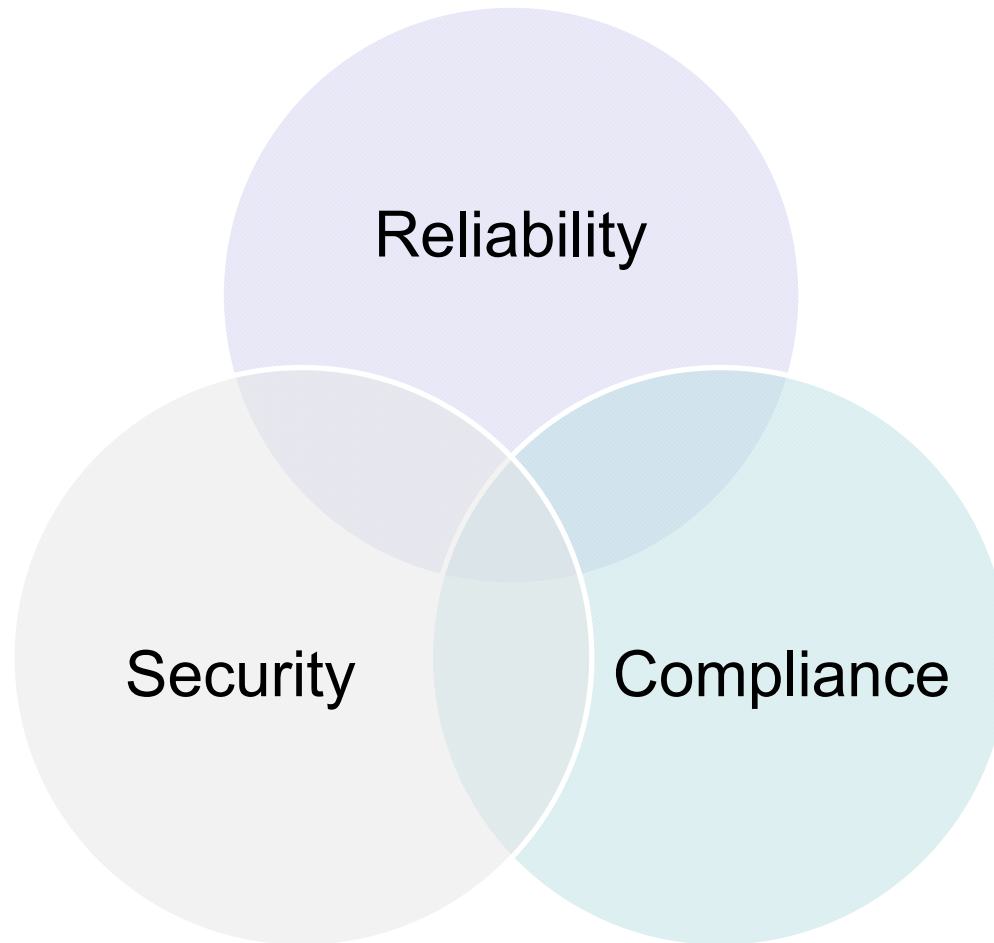
Sustaining Compliance...

- Make compliance immediately apparent
- Be able to demonstrate the “5 Ws”
- Be able to **tell** the auditor how you meet the requirement (protocol)
 - Often policy, process, procedure, etc
- Be able to **show** the auditor that you are actually meeting the requirement (proof)
 - Often supporting evidence such as logs, spreadsheets, documents, database extracts, captures, etc

Potential Obstacles

- The middle management filter
- The ostrich factor
- The litigation option
- Budget, resources, convenience
- Vendors
- Consultants
- Moving target

The Big Picture



Questions?

Patrick Miller

CISA, CISSP-ISSAP, SSCP, CEH, NSA-IAM...

Sr. Compliance Engineer, Cyber Security

Western Electricity Coordinating Council

7600 NE 41st Street, Suite 160

Vancouver, WA 98662

360.567.4056 (d) | 503.260.6472 (m)

pmiller@wecc.biz

