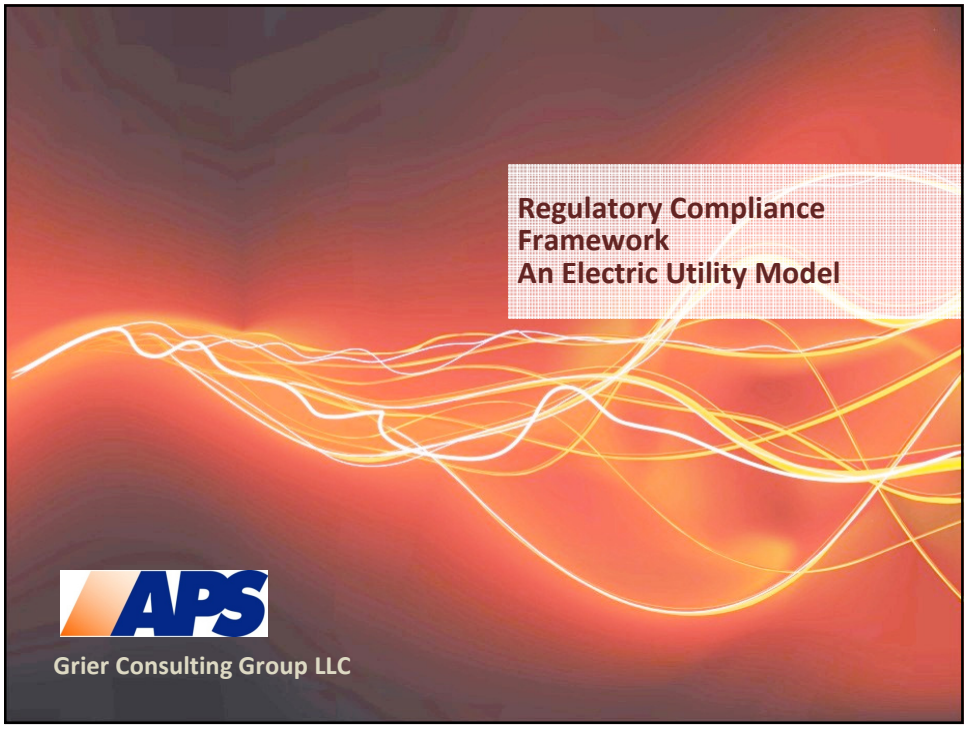


Abstract

This presentation will describe the development of a regulatory compliance framework and toolset for use by a utility regulatory services department. The framework was developed to help the utility to identify, risk assess, manage and control the variety of policies, standards, orders and requirements of federal, regional, and state regulatory commissions and agencies. The compliance framework was based on selected segments of the Committee of Sponsoring Organizations ("COSO") framework standard. These include:

1. Requirement Identification - The catalog of specific external compliance requirement elements against the applicable FERC, NERC, Regional ERO, state public utility, and CFTC standards, orders, rules, and other requirements;
2. Risk Assessment - How to define the inherent and residual risks associated with each compliance requirement and how these risks are analyzed;
3. Control Activities - An approach to the policies and procedures which are necessary to implement the framework and to ensure that risk mitigations (commitments) are effectively carried out;
4. Information and Communication - How to identify, capture, and communicate appropriate information to internal personnel in a timeframe that enables people to carry out their compliance responsibilities; and
5. Monitoring - Plans for ongoing monitoring of the compliance framework.

In addition, the presentation will describe a risk ranking approach and directional scale to allow an assessment of compliance maturity, as well as the expected likelihood and impact of non-compliance across all in-scope compliance areas.

Outline

- The US Electric Utility Industry – A Snapshot
- Electric Utility Compliance – The Scope and Scale of the Challenge
- COSO – The Basis of a Compliance Framework Model
- A Simple Compliance Process (KISS)
- A Role for Technology
- Conclusions

Electric Utility Industry
A Snapshot

The US Electric Utility Industry – A Snapshot

Revenue from Ultimate Sales (2005)	**$342 B[1]**
Employment	**400,000[1]**
U.S. Electric Utility Market Structure[1]	**72% - Investor Owned** **12% - Cooperatives** **11% - Municipal Systems** **5% - Other**
Investor Owned Electric Utility Market Capitalization	**+ $562 B[2]**

Sources: 1. Edison Electric Institute
2. Yahoo Finance (February 10, 2009)

Electric Utility Compliance
The Scope and Scale of the Challenge

An Electric Utility May Be Under Compliance Requirements from a Large Variety of Federal, Regional, and State Regulatory Agencies

Western Electricity Coordinating Council

For Example, The Federal Electric Reliability Standards Demonstrate the Scope and Scale for a Single Set of Compliance Requirements

- **FERC Regulates Electric Reliability under US 18 CFR Part 40**
- **Penalties for Non-Compliance to Electric Reliability Standards May Be $1M per day Per Occurrence**

- **The North American Electric Reliability Corporation oversees the reliability of the bulk power system in North America**
- **Currently 110 Standards representing over 1,800 specific requirements**

Western Electricity Coordinating Council

- **Regional Reliability Organizations are Charged With Monitoring Utilities in Meeting the Standard's Requirements**

Electric Utility — **Must Be "Auditably Compliant" to 100's of Applicable Requirements 24 - 7, 365 Days Per Year**

COSO
The Basis of a Compliance Framework Model

COSO ERM – The Basis for A Compliance Framework Model

1. Grier Consulting Group analysis of Enterprise Risk Management – Integrated Framework, Committee of Sponsoring Organizations (COSO) of the Treadway Commission, 2004.

Assess Operating Environment – setting the basis for how the organization views compliance.

Set Compliance Objectives – defining appropriate compliance objectives.

Identify Compliance Obligations – internal and external compliance events.

Assess Noncompliance Risk – on an inherent and a residual basis.

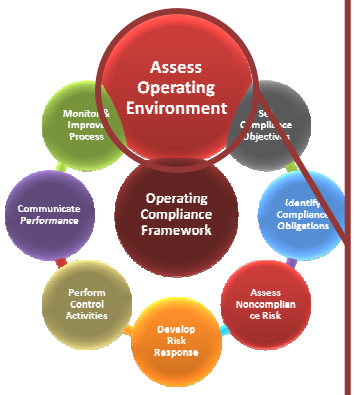
Develop Risk Response – management's set of actions.

Perform Control Activities – ensure responses are effectively carried out.

Communicate Performance – appropriate form and timeframe.

Monitor and Improve Performance – the compliance management process is monitored and modifications made as necessary.

Model Compliance Framework – Assessing the Operating Environment



Assess Operating Environment

- Understand how compliance might be viewed by the organization and provide the appropriate communication and guidance to ensure the organization meets the expectations of management.
- Determine and establish the appropriate governance structures.
- Identify the appropriate risk management philosophy associated with the compliance (may or may not be well defined by the regulator).

Model Compliance Framework – Set Compliance Objectives

Set Compliance Objectives

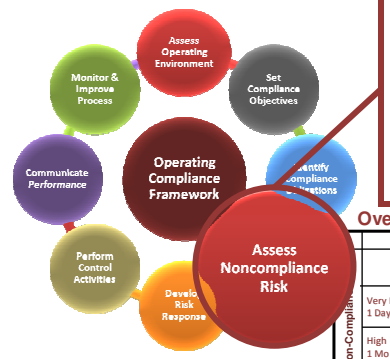
- Management's clearly state compliance objectives.
- The processes developed to support and align management's compliance objectives.
- The set of workflows which represent appropriate processes to support the compliance process.

Model Compliance Framework – Identify Compliance Obligations

Identify Compliance Obligations

- Each requirement set out in federal and state law and regulation are assessed for their potential for the risk of non-compliance (each potential non-compliance is an event).
- Determine the impacted organization (is it across the enterprise, multiple, or single business unit?)

Model Compliance Framework – Assess Non-Compliance Risk



Assess Non-Compliance Risk

- Risk – The detrimental effect a violation of the requirement could have on the organization (typically measured as, **High** **Medium**, and **Lower**).

Overall Red, Amber, Green (RAG) Status in $ per Day Impact

Likelihood of Non-Compliance	Estimated Impact of Non-Compliance (Total $)				
	Very Low $0 → $50K	Low $50K → $500K	Medium $500K → $1M	High $1M → $10M	Very High $10M → $100M
Very High 1 Day → 1 Mo	$208	$833	$3,123	$10,411	$208,219
High 1 Mo → 1 Yr	$14	$55	$205	$685	$13,699
Medium 1 Yr → 5 Yrs	$2	$28	$104	$347	$6,944
Long 5 Yrs → 20 Yrs	$2	$7	$25	$83	$1,667
Very Long 20 Yrs → 100 Yrs	$0	$1	$5	$17	$347

Inherent Risk – Defined as the product of likelihood and impact to a negative event on the organization without any use of appropriate risk management techniques.

Model Compliance Framework – Develop Risk Response

Develop Risk Response

- Performed as a result of the risk assessment and, when complete, provides a new condition to be assessed relative to compliance requirements.
- Maintain a process for determining appropriate mitigation responses to any level of event non-compliance.
- Manage all commitments made to remediate identified non-compliance items.

Model Compliance Framework – Control Activities

Perform Control Activities

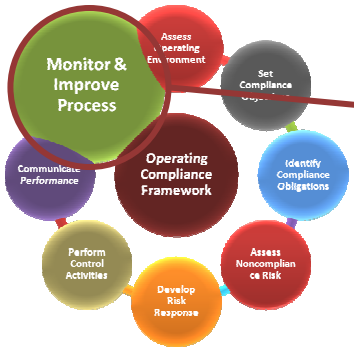
- Policies and procedures established and implemented to help ensure the risk responses are effectively carried out.
- The organization (e.g., Internal Audit) should provide appropriate control testing of the compliance management program.

Model Compliance Framework – Communicate Performance

Communicate Performance

- Use of a "compliance management tool" (CMT) and related processes provide a vehicle for the identification, capture and communication of important information relative to compliance.
- The CMT allows large volumes of compliance items to be assessed and managed.
- Those who are responsible for managing the governing rules, regulations, requirements, risk controls and risk mitigation can use the CMT to identify at a glance which risks require additional mitigation and control.

Model Compliance Framework – Monitor and Improve Performance

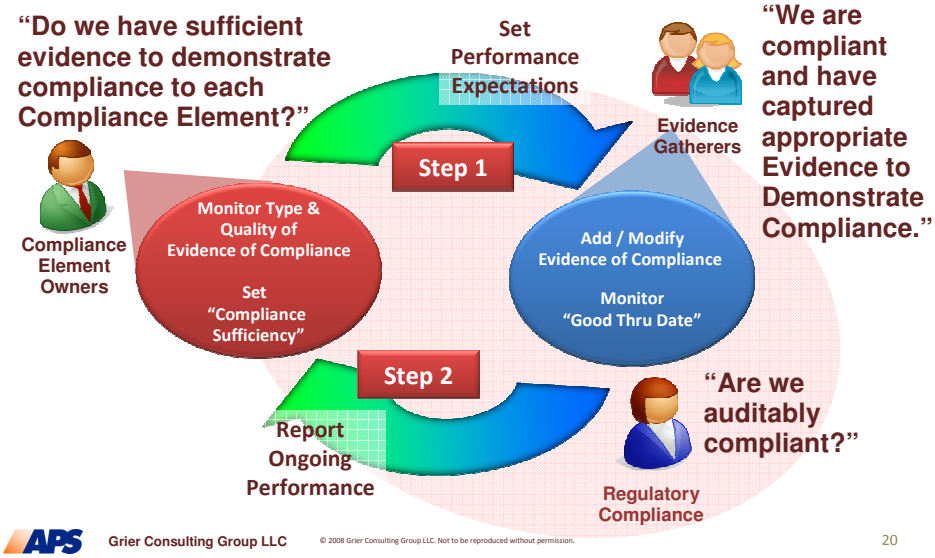


Monitor and Improve Performance

- The entirety of the compliance management program is monitored and modifications made as necessary.
- Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

A Simple Compliance Process (KISS)

A Simple Compliance Process – Two Steps



Compliance Framework Process
Roles and Responsibilities

Compliance Element Owners

- **Monitor Standards Compliance** (Are we doing the Right Things?)
- **Review Evidence of Compliance** (Are we able to show we are Doing the Right Things?)
- **Set "Compliance Sufficiency"** (Are we ready for an Audit?)
- **Effectively Support Regulatory Compliance Efforts** (Reviews and Audits)

Evidence Gatherers

- **Understand the Requirements** (What does "Doing the Right Thing" mean?)
- **Execute to the Requirements** (Doing the Right Thing.)
- **Capture Evidence** (Demonstrate we are Doing the Right Thing.)
- **Maintain Compliance Diligence** (Does evidence still provide appropriate substantiation?)

Regulatory Compliance

- **Primary Compliance Interface** (To the regulator)
- **Provide Compliance Support** (Governance, Process, Tools)
- **Monitor Performance** (Heads-Up Reports, Aging Reports, etc.)
- **Report to Management** (Are we prepared to show that we are in "Auditably Compliant"?)

A Role for Technology

Thoughts on Technology Solution

- Familiar technology platform – friendly to large number of users
- Processes and workflows established and facilitated by experts to drive consistency
- Intuitive user interface simplifying training
- Extensive use of pull-down menus or radio buttons to support consistency of assessment input
- Utilization of “dashboards” to monitoring and review performance

Conclusions

Conclusions

- The public's desire for more transparency has led the regulator to promulgate more compliance requirements
- Scope and Scale are becoming so complex that ad-hoc monitoring of compliance is no longer realistic
- COSO can provide a recognized compliance framework model
- The compliance entity (utility) must:
  - Define what a "Compliance Event" means to them
  - Depend on a simple process to address each Compliance Event
  - Provide overall monitoring of the Compliance Framework for effectiveness and be able to modify when it is not working
- Technology can play an important role in managing large, diverse, systems of compliance requirements

Contact details:

APS

Linda Thompson

Arizona Public Service Co.

Director – Ethics and Compliance

602-250-2366

Linda.Thompson@aps.com

Grier Consulting Group LLC

Chris Grier

President

480-282-0150

chris.grier@grierconsulting.com