A Progressive Vision for Security and Compliance

Presented By:
Shelley Cottrill
CPA, CSOX, CGRC
ALLEGHENY ENERGY
Allegheny Energy – A snapshot

- Employees: 4,000
- Revenues: $3 Billion
- Headquarters: Greensburg, PA
- NYSE: AYE
- Vertically Integrated Electric Utility: Regulated and Unregulated operating holdings:
  - Allegheny Energy Supply
  - Allegheny Power
    - West Penn Power Company
    - Monongahela Power Company
    - The Potomac Edison Power Company
Utilities’ Imperative for Security

• **Protection of Operating Assets and Reliability**
  – Securing Cyber Critical Assets (CCAs)
  – Securing safety systems for key grid components
  – Ensuring continuity of operations and mitigating risks of revenue interruption

• **Regulatory Compliance**
  – Cost and complexity of regulations is growing
  – Imperative to implement risk-based continuous compliance
Regulations for Utilities

• State regulatory agencies
• Federal regulatory agencies
• Competitive Practices
• Lobbying
• E-Compliance
• Information Management
• Emergency Response

• Employment and Labor
• Financial / SOX
• Ethics
• Environmental, Health and Safety
• CFTC (Futures Trading)
• Financial / SEC
Security and Compliance Challenges

• Number of regulations are growing; heavy fines for non-compliance
• Business participation in compliance, risk and security processes (including SAP) is low or non-existent due to complexity
• Manual, costly and labor intensive path to compliance and security
• Too many silos of data, disconnected processes
• Auditors are more demanding
• Brand and reputation remain at risk
Life in the Trenches Today

• Point-solution for each regulation is costly
• Sustainability - Controls testing and audit functions duplicated for each regulation
• Control Documentation Solutions are not integrated with SAP and other ERPs
• Integration of systems across the grid is creating privacy and data leakage scenarios
• Manual testing of controls is painful, time consuming, error-prone and not scalable
Progressive Vision for Security and Compliance

- Build Continuous Compliance built into the process
- Incorporate New Regulations – AMI SEC standards etc.
- Uncover previously un-detectable security risks
- Implement Security Convergence of IT Systems, Physical Access and Control Systems
- Eliminate silos, lower cost of compliance and slash audit costs
- Active Policy Enforcement
Can your business people find and fix risk in the following? This is one of the major reasons for high TCO and lack of sustainability.

<table>
<thead>
<tr>
<th>Risk Description</th>
<th>Level</th>
<th>Permission Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>BO0100501 Basis</td>
<td>Medium</td>
<td>Transaction Code Check at</td>
</tr>
<tr>
<td>Development &amp;</td>
<td></td>
<td>Transaction Start</td>
</tr>
<tr>
<td>System Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BO0100501 Basis</td>
<td>Medium</td>
<td>Transaction Code Check at</td>
</tr>
<tr>
<td>Development &amp;</td>
<td></td>
<td>Transaction Start</td>
</tr>
<tr>
<td>System Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BO0100501 Basis</td>
<td>Medium</td>
<td>S.DEVELOP : ABAP Workbench</td>
</tr>
<tr>
<td>Development &amp;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BO0100501 Basis</td>
<td>Medium</td>
<td>S.ADM/LFC : System</td>
</tr>
<tr>
<td>Development &amp;</td>
<td></td>
<td>Authorization</td>
</tr>
<tr>
<td>System Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BO0100501 Basis</td>
<td>Medium</td>
<td>S.ADM/LFC : System</td>
</tr>
<tr>
<td>Development &amp;</td>
<td></td>
<td>Authorization</td>
</tr>
<tr>
<td>System Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BO130HG01 Archiving &amp; System Administration</td>
<td>Medium</td>
<td>Transaction Code Check at Transaction Start</td>
</tr>
<tr>
<td>BO130HG01 Archiving &amp; System Administration</td>
<td>Medium</td>
<td>Transaction Code Check at Transaction Start</td>
</tr>
<tr>
<td>BO130HG01 Archiving &amp; System Administration</td>
<td>Medium</td>
<td>S.ADM/LFC : System Authorization</td>
</tr>
</tbody>
</table>
SAP Security Visuals for FERC Compliance
Business Visuals for SOX Compliance
Critical Assets and Risks Identified Visually

Risk: Terminated Employee has access to SCADA

- Terminated users have active access to the SCADA system.
- SOA Risk-Able to modify relays through SCADA and change access to PI Historian.
- Critical configuration changes can be performed by a single user.
- Terminated users have active physical access to the SCADA system.
- Valid remote access to non-employees with admin privileges.
Access Revoked Instantly

Risk Remediation for risk NERC CIP006-R1, CIP004-R2 for personnel Dave Jackson has been successfully performed. A request has been created to complete the process.

Risk: CIP006R15-002 - Terminated Personnel have valid physical access to critical cyber assets.
Level: High
Compliance Requirements: NERC CIP006-R1, CIP004-R2
Violations: 10
Impact: Personnel can gain unauthorized access to critical cyber assets leading to sabotage hurting the reliability of the Bulk Electric System (BES).
Business Process: Transmission Operations
Risk Owner: Tom McGuire

Details:

<table>
<thead>
<tr>
<th>User</th>
<th>Position</th>
<th>System</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dave Jackson</td>
<td>SCADA Operator</td>
<td>SanJose GE PP</td>
<td>Sub-station Control Room</td>
</tr>
<tr>
<td>Mike Singer</td>
<td>Load Analyst I</td>
<td>SanJose GE PP</td>
<td>Transmission Switch Yard</td>
</tr>
<tr>
<td>John Smith</td>
<td>Inter-connect Manager</td>
<td>SanJose GE PP</td>
<td>Sub-station Control Room</td>
</tr>
<tr>
<td>Mark Doe</td>
<td>Load Analyst III</td>
<td>Corporate Honeywell</td>
<td>Transmission Switch Yard</td>
</tr>
<tr>
<td>Lisa Ray</td>
<td>Generator Mechanic</td>
<td>Corporate Honeywell</td>
<td>Generator / Control Center</td>
</tr>
</tbody>
</table>

Remediate Risk  Mitigate Risk  Forward  Back
Active Policy Enforcement

• Solution identifies terminated employees and correlates to SCADA Access Violations
• NERC CIP Policy mandates removal of access within 24-hours
• Built-in rule engine incorporates policy into application
• Application enforces policy by allowing situation managers to remove access in real-time
Allegheny’s Risk-Based Approach Delivers Security and Compliance

• Continuous visibility into risk
• Compliance built into the process
• Easily change / add new regulations
• Uncover previously un-detectable risks
  – IT Systems, Physical Access and Control Systems
• Active Policy Enforcement
• Eliminate silos, reduces cost of audit and compliance
Thank You

Shelley Cottrill
Scottrri@alleghenyenergy.com