The Risk Management Process (RMP) initiative is a public-private collaboration to develop a cybersecurity risk management guideline.

This work is led by DOE in coordination with NIST and NERC, and includes representatives from the public and private sectors.

- Utilities are nominated by APPA, EEI, and NRECA and form the core team
- DOE, NIST, NERC, SGIP-CSWG, DHS and FERC are also part of the core team
- A subject matter expert (SME) team is composed of utility representatives and other stakeholders to provide additional guidance to the team
So What is the RMP About?

• It’s about people and the organizations in which they operate
  – How to organize people to effectively make risk informed decisions
  – Target of RMP is cybersecurity risk but fundamentally could be applied to any risk management domain

Electricity subsector organizations deal with risk every day in meeting their business objectives...this management of risk is conducted as an interactive, ongoing process as part of normal operations.
Guiding Principles of the RMP

• Based on NIST 800-39: Managing Information Security Risk

• Describe “what” not “how”

• Adaptable to any size or type of organization

• Cybersecurity alignment with mission and business processes
The Risk Management Model is a three-tiered structure that provides a comprehensive view of an organization.

It provides a structure for how cybersecurity risk management activities are undertaken across an organization.

Strategy is communicated down through the organization, risk evaluations are communicated up.
RMP Overview: Risk Management Cycle

- The Risk Management Cycle provides four elements that structure an organization’s approach to cybersecurity risk management.
- The Risk Management Cycle is not static but a continuous process, constantly re-informed by the changing risk landscape as well as by organizational priorities and functional changes.
RMP Overview: Risk Management Cycle cont’d

• Risk Framing
  – Describes the environment in which decisions are made
  – Assumptions, constraints, tolerance, priorities

• Risk Assessment
  – Identify, prioritize, and estimate risk to organization
  – Includes supply chain and external service providers

• Risk Response
  – How the organization responds to risk
  – Develop courses of action and implement

• Risk Monitoring
  – How risks are monitored and communicated over time
  – Verify and evaluate risk response measures
The Risk Management Process is the application of the risk management cycle to each of the tiers in the risk management model.
RMP Overview: Information Flowchart

Figure 4: RMP Information Flowchart

TIER 1: Executive Leadership
- Corporate strategy
- Policy

TIER 2: Business Management
- Actionable policy and procedures
- Guidance and constraints

TIER 3: Systems Management
- Results of monitoring
- Feedback

- Results of monitoring
- Feedback
Tier 1: Organization
Risk Framing

**INPUTS**
- Mission and vision statement
- Legislation
- Organizational policies
- Regulatory requirements
- Contractual relationships
- Financial limitations
- Trust relationships
- Organizational culture
- Governance structures
- Output from Tier 1 risk monitoring element
- Feedback from Tier 2 risk management cycle

**ACTIVITIES**
- Define risk assumption
  - Threat sources
  - Vulnerabilities
  - Impact
  - Likelihood
- Identify risk management constraint
- Determine and implement risk tolerance
- Identify priorities
- Develop Risk Management Strategy

**OUTPUTS**
- Risk Management Strategy
Tier 1: Organization Risk Assessment

**INPUTS**
- Risk assessment methodology
- Assessment of external service providers
- Risk aggregation methodology
- Outputs from Tier 1 risk framing element

**ACTIVITIES**
- Identify threats and vulnerabilities
- Determine risk

**OUTPUTS**
- Determination of risk for the organization
## Tier 1: Organization Risk Response

<table>
<thead>
<tr>
<th>INPUTS</th>
<th>ACTIVITIES</th>
<th>OUTPUTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk assessment</td>
<td>Identify risk response</td>
<td>Risk response plan</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>- Risk acceptance</td>
<td></td>
</tr>
<tr>
<td>Risk response guidance from the organization’s Risk Management Strategy</td>
<td>- Risk avoidance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Risk mitigation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Risk sharing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Risk transference</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Combination</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Evaluate alternatives</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Determine and implement risk response</td>
<td></td>
</tr>
</tbody>
</table>
Tier 1: Organization Risk Monitoring

**INPUTS**
- Information on industry best practices, tools, and frequency
- Cybersecurity governance structure
- Performance information
- Comprehensive lists of identified risks

**ACTIVITIES**
- Develop risk monitoring strategy
  - Monitoring implementation
  - Monitoring effectiveness
  - Monitoring changes
  - Automated versus manual monitoring
  - Frequency of monitoring
  - Monitor risk

**OUTPUTS**
- Validation of existence and effectiveness of risk response measures
- Identification of changes to IT and ICS and their environments of operation
- Risk monitoring strategy
## Tier 1: Organization Summary

<table>
<thead>
<tr>
<th>INPUTS</th>
<th>ACTIVITIES</th>
<th>OUTPUTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RISK FRAMING</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mission and vision statement</td>
<td>Define risk assumption</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>Legislation</td>
<td>Threat sources</td>
<td></td>
</tr>
<tr>
<td>Organizational policies</td>
<td>Vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>Regulatory requirements</td>
<td>Impact</td>
<td></td>
</tr>
<tr>
<td>Contractual relationships</td>
<td>Likelihood</td>
<td></td>
</tr>
<tr>
<td>Financial limitations</td>
<td>Identify risk constraint</td>
<td></td>
</tr>
<tr>
<td>Trust relationships</td>
<td>Determine and implement risk tolerance</td>
<td></td>
</tr>
<tr>
<td>Organizational culture</td>
<td>Identify priorities</td>
<td></td>
</tr>
<tr>
<td>Governance structures</td>
<td>Develop Risk Management Strategy</td>
<td></td>
</tr>
<tr>
<td>Output from Tier 1 risk monitoring element</td>
<td>Feedback from Tier 2 risk management cycle</td>
<td></td>
</tr>
</tbody>
</table>

| RISK ASSESSMENT | | |
| Risk assessment methodology | Identify threat and vulnerability | Determination of risk for the organization |
| Assessment of external service providers | Determine risk | |
| Risk aggregation methodology | | |
| Outputs from Tier 1 risk framing element | | |

| RISK RESPONSE | | |
| Risk assessment | Identify risk response | Risk response plan |
| Vulnerabilities | Risk acceptance | |
| Risk response guidance from the organization’s Risk Management Strategy | Risk avoidance | |
| | Risk mitigation | |
| | Risk sharing | |
| | Risk transference | |
| | Combination | |

| RISK MONITORING | | |
| Information on industry best practices, tools, and frequency | Develop risk monitoring strategy | Validation of existence and effectiveness of risk response measures |
| Cybersecurity governance structure | Monitoring implementation | |
| Performance information | Monitoring effectiveness | |
| Comprehensive lists of identified risks | Monitoring changes | |
| | Automated versus manual monitoring | Identification of changes to IT and ICS and their environments of operation |
| | Frequency of monitoring | Risk monitoring strategy |
| | Monitor risk | |

Office of Electricity Delivery and Energy Reliability
## Tier 2: Mission and Business Process Risk Framing

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Activities</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outputs from Tier 1:</td>
<td>Identify mission and business processes and applications</td>
<td>Identification of the mission and business processes</td>
</tr>
<tr>
<td>- Mission objectives</td>
<td>Establish risk tolerance and risk methodology</td>
<td>Documented lists of the impacts</td>
</tr>
<tr>
<td>- Risk Management Strategy</td>
<td>Identify cybersecurity program and architecture</td>
<td>Documented risk assessment methodologies</td>
</tr>
<tr>
<td>- Governance structure</td>
<td>Develop or refine enterprise architecture</td>
<td>Process-specific risk tolerances</td>
</tr>
<tr>
<td>- High-level security requirements</td>
<td></td>
<td>An inventory of applications, classifications, and owners that support mission and business processes</td>
</tr>
<tr>
<td>- Risk management constraints</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Risk tolerance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feedback from risk monitoring element at Tier 2 and Tier 3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Tier 2: Mission and Business Process Risk Assessment

**INPUTS**
- Risk Management Strategy from Tier 1
- Reports from threat and vulnerability sources identified in Tier 1 and at the process-specific risk framing element in Tier 2
- Selected risk assessment methodologies from the framing element in Tier 2
- Inputs from previous Tier 2 risk assessments and feedback from Tier 3 monitoring element
- Inventory of mission and business processes and information systems from the framing element of Tier 2
- List of the impacts associated with the loss of confidentiality, integrity, and availability of mission and business process information, data elements, IT and ICS

**ACTIVITIES**
- Prioritize mission and business processes based on consequence/impact
- Determine risk

**OUTPUTS**
- A mission and business process list prioritized by impact
- Specific threat and vulnerability information generated at Tier 2 that is used for the development of the cybersecurity program and architecture
### Tier 2: Mission and Business Process Risk Response

<table>
<thead>
<tr>
<th>INPUTS</th>
<th>ACTIVITIES</th>
<th>OUTPUTS</th>
</tr>
</thead>
</table>
| - Risk Management Strategy from Tier 1  
- Tier 1 business processes risk tolerance  
- Tier 2 mission and business process list prioritized by impact  
- Risk management constraints from Tier 1 and Tier 2  
- Cybersecurity and enterprise architectures  
- Threat and vulnerability information identified in the Tier 2 risk assessment activities | - Determine and implement risk response  
- Define cybersecurity program and architecture  
  - Guiding principles  
  - Requirements  
  - Processes  
  - Strategies | - Cybersecurity program, including policies, standards, and procedures  
- Cybersecurity architecture |
Tier 2: Mission and Business Process

Risk Monitoring

**INPUTS**
- Risk Management Strategy from Tier 1
- Cybersecurity program and architecture
- Results of previous audits and assessments
- Cybersecurity reporting from Tier 2 and Tier 3
- Threat and vulnerability industry alerts and warnings
- Outputs from the Tier 2 risk response element

**ACTIVITIES**
- Establish metrics to measure conformance to cybersecurity architecture
- Measure effectiveness of cybersecurity architecture
- Periodically reassess cybersecurity architecture
- Monitor changes to environment

**OUTPUTS**
- Risk monitoring reports from the conformance and effectiveness reviews and appropriate resulting mitigations and changes
- A risk monitoring strategy embedded in the cybersecurity program, which includes metrics, frequency, and scope of the monitoring processes
## Tier 2: Mission and Business Process Summary

<table>
<thead>
<tr>
<th>Risk Framing</th>
<th>Inputs</th>
<th>Activities</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Outputs from Tier 1:</td>
<td>- Mission objectives</td>
<td>- Identify mission and business processes and information systems</td>
<td>- Identification of the mission and business processes</td>
</tr>
<tr>
<td>- Risk Management Strategy</td>
<td>- Governance structure</td>
<td>- Establish risk tolerance and risk methodology</td>
<td>- Documented lists of the impacts</td>
</tr>
<tr>
<td>- High-level security requirements</td>
<td>- Risk management constraints</td>
<td>- Identify cybersecurity program and architecture</td>
<td>- Documented risk assessment methodologies</td>
</tr>
<tr>
<td>- Risk tolerance</td>
<td>- Feedback from risk monitoring element at Tier 2 and Tier 3</td>
<td>- Develop or refine enterprise architecture</td>
<td>- Process-specific risk tolerances</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Assessment</th>
<th>Inputs</th>
<th>Activities</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Risk Management Strategy from Tier 1</td>
<td>- Reports from threat and vulnerability sources identified in Tier 1 and all the process-specific risk framing element in Tier 2</td>
<td>- Prioritize mission and business processes based on consequence/impact</td>
<td>- A mission and business process list prioritized by impact</td>
</tr>
<tr>
<td>- Tier 1 business processes risk tolerance</td>
<td>- Selected risk assessment methodologies from the framing element in Tier 2</td>
<td>- Determine risk</td>
<td>- Specific threat and vulnerability information generated at Tier 2 that is used for the development of the cybersecurity program and architecture</td>
</tr>
<tr>
<td>- Tier 2 mission and business process list prioritized by impact</td>
<td>- Inputs from previous Tier 2 risk assessments and feedback from Tier 3 monitoring element</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Risk management constraints from Tier 1 and Tier 2</td>
<td>- Inventory of mission and business processes and information systems from the framing element of Tier 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Cybersecurity and enterprise architectures</td>
<td>- List of the impacts associated with the loss of confidentiality, integrity, and availability of mission and business process information, data elements, IT and ICS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Response</th>
<th>Inputs</th>
<th>Activities</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Risk Management Strategy from Tier 1</td>
<td>- Tier 1 business processes risk tolerance</td>
<td>- Determine and implement risk response</td>
<td>- Cybersecurity program including policies, standards, guidelines, and procedures</td>
</tr>
<tr>
<td>- Tier 2 mission and business process list prioritized by impact</td>
<td>- Risk management constraints from Tier 1 and Tier 2</td>
<td>- Define cybersecurity program and architecture</td>
<td>- Cybersecurity architecture</td>
</tr>
<tr>
<td>- Cybersecurity and enterprise architectures</td>
<td>- Threat and vulnerability information identified in the Tier 2 risk assessment activities</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Monitoring</th>
<th>Inputs</th>
<th>Activities</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Risk Management Strategy from Tier 1</td>
<td>- Cybersecurity program and architecture</td>
<td>- Establish metrics to measure the conformance to cybersecurity architecture</td>
<td>- Risk monitoring reports from the effectiveness and efficiency reviews and appropriate resulting mitigations and changes</td>
</tr>
<tr>
<td>- Cybersecurity and enterprise architectures</td>
<td>- Results of previous audits and assessments</td>
<td>- Measure the effectiveness of cybersecurity architecture</td>
<td>- A risk monitoring strategy embedded in the cybersecurity program, which includes metrics, frequency, and scope of the monitoring processes</td>
</tr>
<tr>
<td>- Threat and vulnerability industry alerts and warnings</td>
<td>- Outputs from the Tier 2 risk response element</td>
<td>- Periodically reassess cybersecurity architecture</td>
<td></td>
</tr>
</tbody>
</table>
Tier 3: IT and ICS
Risk Framing

**INPUTS**
- Risk Management Strategy from Tier 1
- Threat and vulnerability information from Tier 2
- Prioritized list of mission and business processes, and information systems by impact/consequence from Tier 2
- Catalog of cybersecurity controls
- Cybersecurity program and architecture
- Enterprise architecture
- Results from monitoring element of Tier 3
- Inventory of current information systems and resources created at Tier 3

**ACTIVITIES**
- Conduct IT and ICS inventory
- Define or refine cybersecurity plans

**OUTPUTS**
- Baseline cybersecurity plan, which includes the inventory of IT and ICS and identification of boundaries, and the list of threats and vulnerabilities
Tier 3: IT and ICS Risk Assessment

**Inputs:**
- Cybersecurity plan
- Assessment methodology from Tier 2

**Activities:**
- Perform cybersecurity risk assessment
- Develop cybersecurity risk assessment report

**Outputs:**
- Cybersecurity risk assessment report with findings and recommendations
Tier 3: IT and ICS
Risk Response

**INPUTS**
- Cybersecurity plan
- Cybersecurity risk assessment report

**ACTIVITIES**
- Determine and implement risk response
  - Risk acceptance
  - Risk avoidance
  - Risk mitigation
  - Risk sharing
  - Risk transference
  - Combination of the above
- Select and refine cybersecurity controls
- Accept cybersecurity plan
- Develop and implement risk mitigation plan

**OUTPUTS**
- Risk acceptance decision
- Refined cybersecurity plan
- Risk mitigation plan
Tier 3: IT and ICS
Risk Monitoring

**Inputs**
- Cybersecurity program and architecture
- Refined cybersecurity plan
- Risk mitigation plan
- Threat and vulnerability information
- Monitoring methodology from Tier 2

**Activities**
- Manage configurations and changes
- Assess cybersecurity controls
- Monitor new threats and vulnerabilities
- Monitor cybersecurity mitigation plan
- Report cybersecurity status
- Implement decommissioning strategy

**Outputs**
- Status of the mitigation plan and remediation actions
- Refined cybersecurity plan
- Refined cybersecurity program and architecture
- Refined monitoring strategy for Tier 2 and Tier 1
## Tier 3: IT and ICS Summary

<table>
<thead>
<tr>
<th>INPUTS</th>
<th>ACTIVITIES</th>
<th>OUTPUTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1 Risk Management Strategy</td>
<td>Conduct IT and ICS inventory</td>
<td>Baseline cybersecurity plan that includes the inventory of IT and ICS and identification of boundaries, and the list of threats and vulnerabilities</td>
</tr>
<tr>
<td>Tier 1 Threat and vulnerability information</td>
<td>Define or refine cybersecurity plans</td>
<td></td>
</tr>
<tr>
<td>Tier 2 Prioritized list of mission and business processes and information systems by impact/consequence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tier 2 Catalog of cybersecurity controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tier 2 Cybersecurity program and architecture</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tier 2 Enterprise architecture</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tier 2 Results from monitoring element of Tier 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tier 2 Inventory of current information systems and resources from Tier 2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Risk Framing
- Cybersecurity plan
- Assessment methodology from Tier 2

### Risk Assessment
- Cybersecurity plan
- Cybersecurity risk assessment report
- Perform cybersecurity risk assessment
- Develop cybersecurity risk assessment report
- Cybersecurity risk assessment report with findings and recommendations

### Risk Response
- Cybersecurity plan
- Cybersecurity risk assessment report
- Determine and implement risk response
  - Risk acceptance
  - Risk avoidance
  - Risk mitigation
  - Risk sharing
  - Risk transference
  - Combination of the above
- Select and refine cybersecurity controls
- Develop and implement risk mitigation plan
- Risk acceptance decision
- Refined cybersecurity plan
- Risk mitigation plan

### Risk Monitoring
- Cybersecurity program and architecture
- Refined cybersecurity plan
- Risk mitigation plan
- Threat and vulnerability information
- Monitoring methodology from Tier 2
- Manage technology acquisition, configuration, and changes
- Assess cybersecurity controls
- Monitor new threats and vulnerabilities
- Monitor cybersecurity mitigation plan
- Report cybersecurity status
- Implement decommissioning strategy
- Status of the mitigation plan and remediation actions
- Refined cybersecurity plan
- Refined cybersecurity program and architecture
- Refined monitoring strategy for Tier 2 and Tier 1
RMP: A Case Study

Scott Saunders, CISSP, CISM, MSISA
Sacramento Municipal Utility District (SMUD)
Why a Case Study

- Transition theoretical ideas into real world
- Create a real word implementation framework
- Validate the RMP
- Provide a “Starting point” for a utility
- Able to highlight opportunities
- Able to highlight struggles
Case Study Directives

• Primary Directive: under 40 pages

• Secondary Directive: fun to read

• Tertiary Directive: weave realism into story
Case Study Characteristics

- Use casual conversation storytelling
- Create characters seen in real utilities
- Create same angst seen in real utilities
- Cover major activities of the RMP
- Reference existing related bodies of work
- Provide example inputs and outputs
- Provides drafting teams own Lessons Learned
## Tier 1: Organization

### Business Impact Assessment

<table>
<thead>
<tr>
<th>Priority</th>
<th>At-Risk Business Functions and Processes</th>
<th>Threats</th>
<th>Vulnerabilities</th>
<th>Impact</th>
<th>Probability</th>
<th>Constraints</th>
<th>Tolerances</th>
<th>Mitigation Action</th>
<th>Next Review Date</th>
</tr>
</thead>
</table>
| 1        | Power Operations                        | Anything that would impact reliability | *Remote access to grid control systems  
*Disruption or corruption of communications | High impact  
*Outages  
*Fines | High | Need to have remote access to systems | We do not want to put reliability of the grid or our delivery of electricity to customers at risk. | Invest in robust protection to make sure that only our staff can get remote access, and are appropriately trained avoid mistakes. |
| 1        | Metering-to-Cash                        | Disruption of systems used to perform fiscal operations or management | *Web site failure | High impact  
*Loss of money, time, and resources to replacement/repair | High | Budget and financial constraints – how much money can be devoted to this effort this year... or future years? | We have to manage our current resources most efficiently. There isn’t more money or more people. | Make sure there are adequate testing of the cybersecurity controls so the websites are resistive to hacking. |
| 1        | Customer Services                       | *Negative press  
*Hacking customer information | *Escalation to regulators | High impact  
*Fines  
*Loss of board confidence | High | State data/PII breach laws | We do not want to have any security breaches that put us in the news or gives the company negative press |  |
## Tier 2: Mission and Business Process Application Inventory

<table>
<thead>
<tr>
<th>Application Inventory</th>
<th>Business Process Supported</th>
<th>Policy / Documentation</th>
<th>Priority</th>
<th>Rank (tier1/tier2)</th>
<th>Impact</th>
<th>Prob.</th>
<th>Risk</th>
<th>Mitigations</th>
<th>Next Review Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMS in the POC Systems</td>
<td>Power Operations - Energy Mgmt</td>
<td>Partial</td>
<td>1</td>
<td>High/ high</td>
<td>High</td>
<td>High</td>
<td>Documentation and security policy</td>
<td>Complete documentation, set policy (Bill_S, Al_K)</td>
<td>July</td>
</tr>
<tr>
<td>Accounting IT- Corp Systems</td>
<td>Metering to Cash - Accounting</td>
<td>Yes - policy</td>
<td>1</td>
<td>High/ med</td>
<td>High</td>
<td>High</td>
<td>Testing and access control</td>
<td></td>
<td>July</td>
</tr>
<tr>
<td>Billing IT- Corp Systems</td>
<td>Metering to Cash - Billing</td>
<td>Yes - policy</td>
<td>1</td>
<td>High/ med</td>
<td>High</td>
<td>High</td>
<td>Missing incident controls</td>
<td></td>
<td>July</td>
</tr>
<tr>
<td>Remote Access Services OT – Systems</td>
<td>Power Operations - Energy Mgmt</td>
<td>Partial</td>
<td></td>
<td>High/ high</td>
<td>High</td>
<td>High</td>
<td>Documentation and security policy</td>
<td>Complete documentation, set policy (Bill_S, Al_K)</td>
<td>July</td>
</tr>
<tr>
<td>Meters - Head in (outsourced) IT- Corp Systems</td>
<td>Metering to Cash - Smart Meters</td>
<td>Outsourced?</td>
<td>2</td>
<td>High/ med</td>
<td>High</td>
<td>Med</td>
<td>Controls at contractor * review contracts</td>
<td></td>
<td>July</td>
</tr>
<tr>
<td>IT Access Control / RSA Type / VPN IT- Corp Systems</td>
<td>Corporate Services</td>
<td>Yes - policy</td>
<td>2</td>
<td>/high</td>
<td>High</td>
<td>Med</td>
<td>Critical service, RSA incident?</td>
<td></td>
<td>July</td>
</tr>
</tbody>
</table>
## Tier 3: IT and ICS

### Systems Inventory

<table>
<thead>
<tr>
<th>Asset Name</th>
<th>Location</th>
<th>Serial Number</th>
<th>MAC Address</th>
<th>IP Address - Network ID - VLAN</th>
<th>System Association</th>
<th>Constraints</th>
<th>Threats / Vulns</th>
<th>Mitigations</th>
<th>Next Review Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE EMS 100 / UNIX Server</td>
<td>Building 2 POC Server Room</td>
<td>492992-0001</td>
<td>N/A</td>
<td>PineOpsNetwork A0023:9000:1</td>
<td>EMS</td>
<td>GE Proprietary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GE EMS 100-A / Controller System / Data Feeds</td>
<td>Building 2 POC Server Room</td>
<td>5600923-2992-0001</td>
<td>N/A</td>
<td>PineOpsNetwork A0023:8567:61</td>
<td>EMS</td>
<td>GE Proprietary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GE DMS Module</td>
<td>Building 2 POC Server Room</td>
<td>A9456-492992-0009</td>
<td>N/A</td>
<td>PineOpsNetwork A0023:6755:12</td>
<td>EMS</td>
<td>GE Proprietary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GE Outage Management Controller</td>
<td>Building 2 POC Server Room</td>
<td>99-854777</td>
<td>N/A</td>
<td>PineOpsNetwork A0023:6928:70</td>
<td>Relay Protection System</td>
<td>GE Proprietary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terminal Services Module</td>
<td>Building 2 POC Server Room</td>
<td>45-78880</td>
<td>N/A</td>
<td>PineOpsNetwork A0023:6999:54</td>
<td>Relay Protection System</td>
<td>GE Proprietary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitor Concentrator</td>
<td>Substations (all)</td>
<td>Varies</td>
<td>N/A</td>
<td>PineOpsNetwork vary</td>
<td>Relay Protection System</td>
<td>GE Proprietary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Item</td>
<td>Date</td>
<td>Action Prescribed</td>
<td>Milestone</td>
<td>Assigned to</td>
<td>Completed</td>
<td>Notes (instructions)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>-------------</td>
<td>-----------</td>
<td>-------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMS in the POC</td>
<td>4-Apr</td>
<td>Complete documentation, set security policy and standards</td>
<td></td>
<td>(Bill_S, Al_K)</td>
<td></td>
<td>Executives: Invest in robust protection to make sure that only our staff can get remote access, and are appropriately trained avoid mistakes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relays &amp; Protected</td>
<td>4-Apr</td>
<td>Complete documentation, set security policy and standards</td>
<td></td>
<td>(Bill_S, Al_K)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Access Services</td>
<td>4-Apr</td>
<td>Complete documentation, set security policy and standards</td>
<td></td>
<td>(Bill_S, Al_K)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Billing</td>
<td>4-Apr</td>
<td>Update policy to address missing incident controls</td>
<td></td>
<td>Monet</td>
<td></td>
<td>Executives: Priority is Metering to Cash</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounting</td>
<td>4-Apr</td>
<td>Update policy to address security testing and access control</td>
<td></td>
<td>Monet</td>
<td></td>
<td>Executives: Priority is Metering to Cash</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What Case Study does not do...

• Cover all business processes in the first implementation
• Prescribe specific methods to perform analysis
• Illustrate all communication issues
• Account for all utility corporate structures
• Include every step and activity in the RMP
RMP: Next Steps

• Publish RMP Case Study
  – Fictional story
  – Illustrates how an organization may implement the RMP

• RMP Pilot
  – Work with 1-3 organizations to implement the RMP
  – Approx. 1 year engagement
  – Capture lessons learned and best practices

• RMP Website
  – Develop a resource center for the RMP
  – Provide additional content
Energy.gov: Office of Electricity Delivery and Energy Reliability


Contact Info:

Matt Light  Marianne Swanson  Scott Saunders
DOE       NIST       SMUD
matthew.light@hq.doe.gov  marianne.swanson@nist.gov  scott.saunders@smud.org