RELIABILITY FIRST

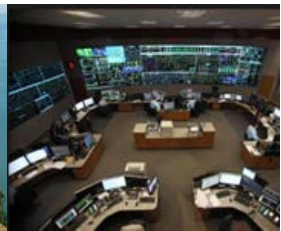
A Case Study

Cyber Security and Compliance

May 2, 2016



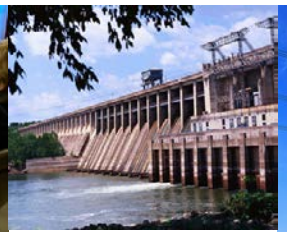


RELIABILITY FIRST

Executive Briefing

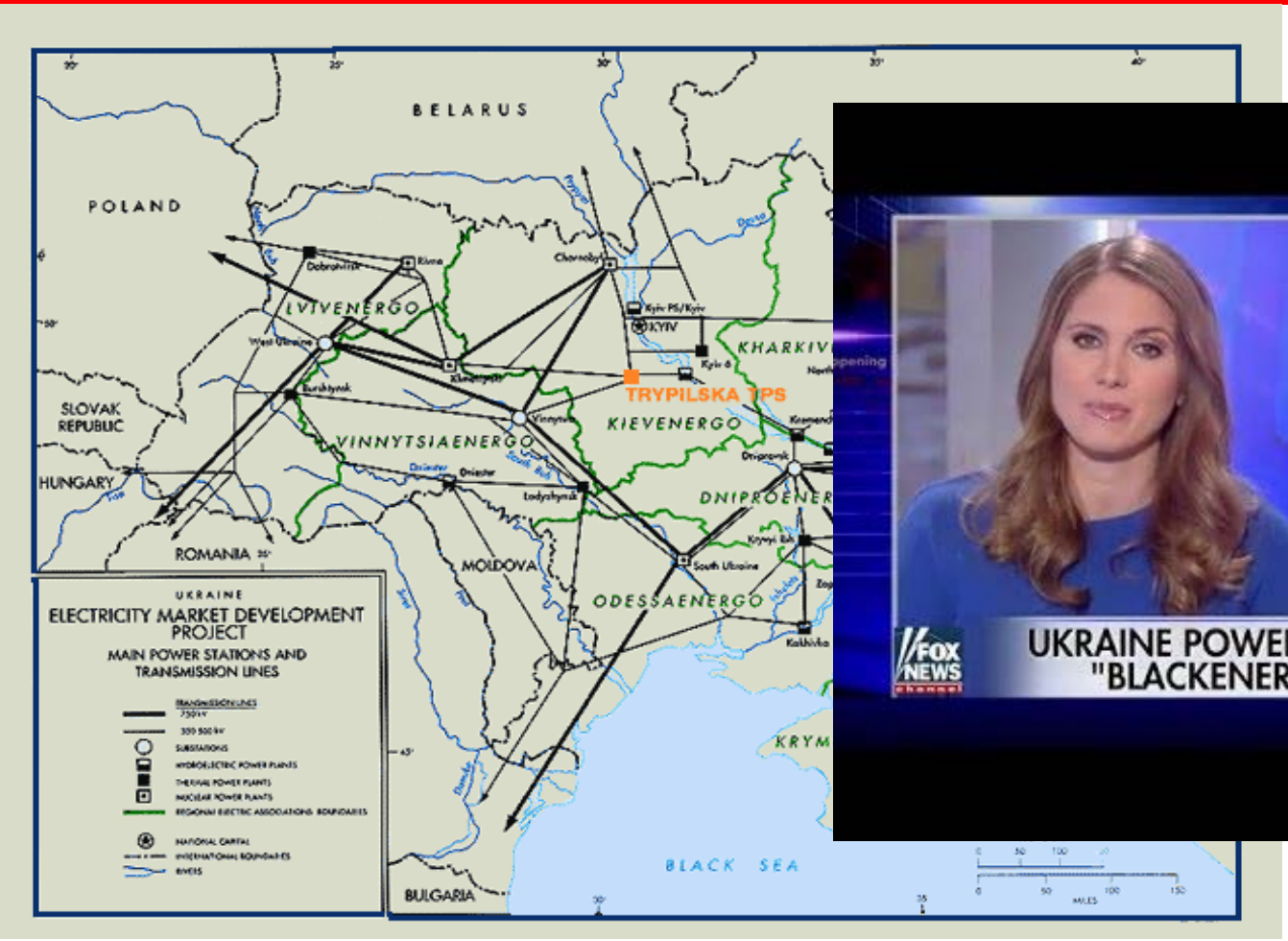
Deandra Williams-Lewis, Director of Enforcement



Security Is Important

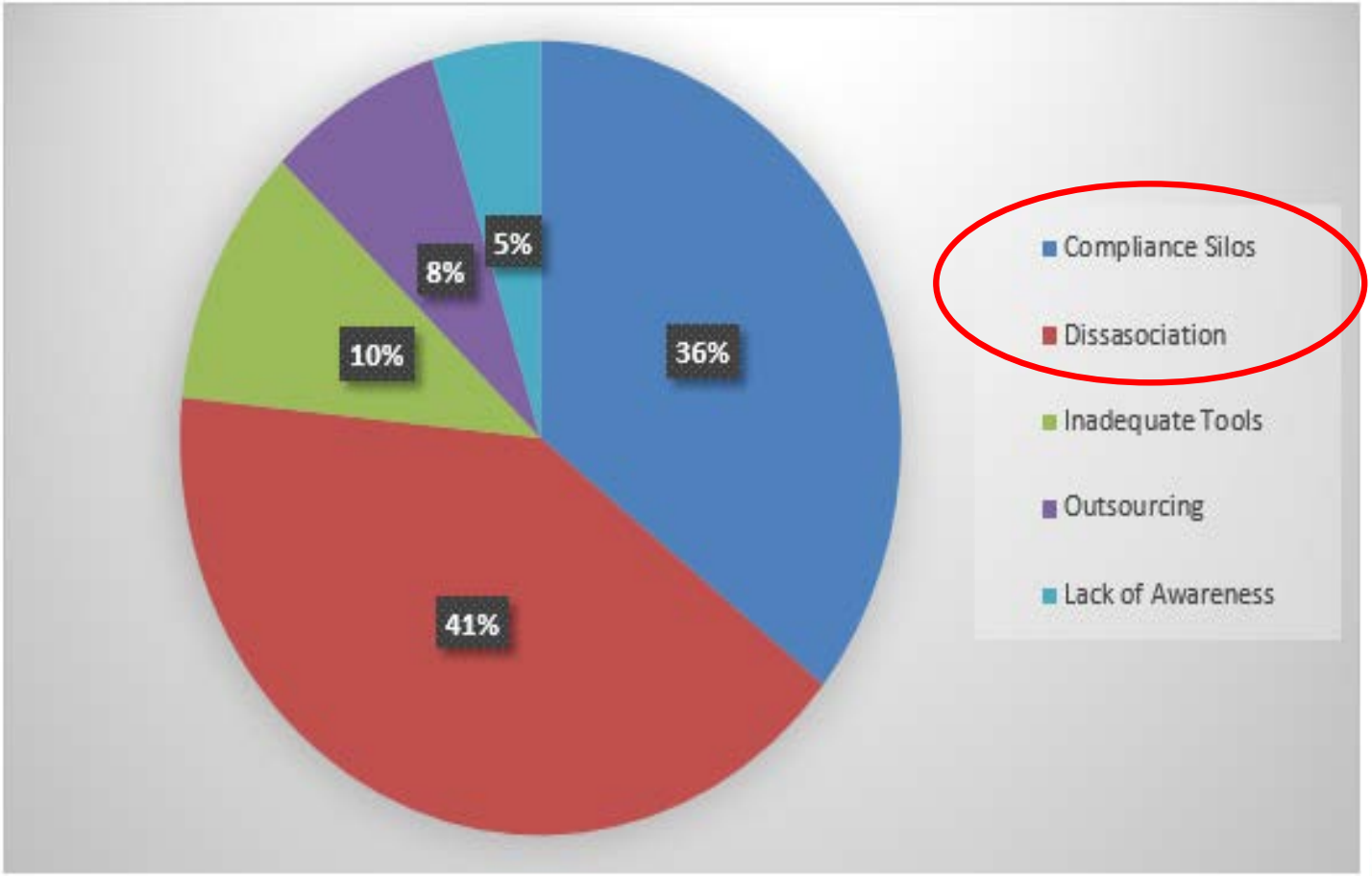
Our Industry Is a Target



"[T]he downing of utilities in western Ukraine on December 23 was due to an attack, which is believed to be the first known successful cyber intrusion to knock a power grid offline."

CIP Themes Report

There are common themes that lead to cultural and programmatic security and compliance issues.



Issue Spotting

- **Reliability Quality Assurance**
  - Independent, Objective Internal Evaluation
- **Ability to Identify, Assess, and Correct**
  - Self-reporting history and expectations
- **Are the Tools Useful?**
  - Benchmark your tools; separate tools for compliance and security?
- **Who, How, and When are You Training?**
  - Timely, Effective, Practical, and Targeted
- **Is your Compliance Dysfunctional?**
  - Attitude towards regulatory governance
- **Implementation Paralysis**
  - Bureaucracy vs. ability to make necessary changes

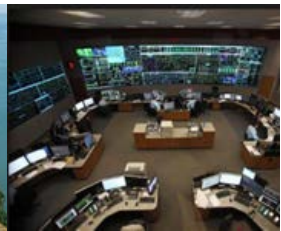
RELIABILITY FIRST

Case Study: East Power

Kristen Senk, Counsel



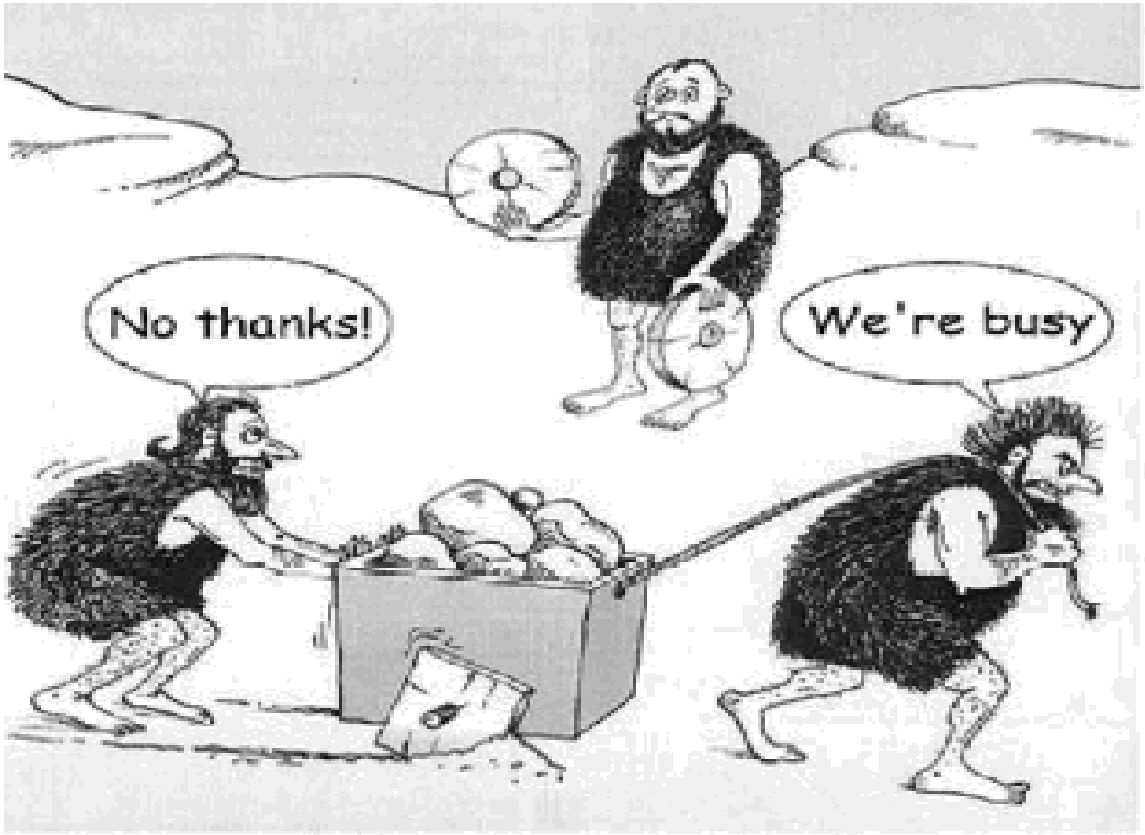


Case Study: East Power

➢ Background

- Audit in 2011: 19 Violations

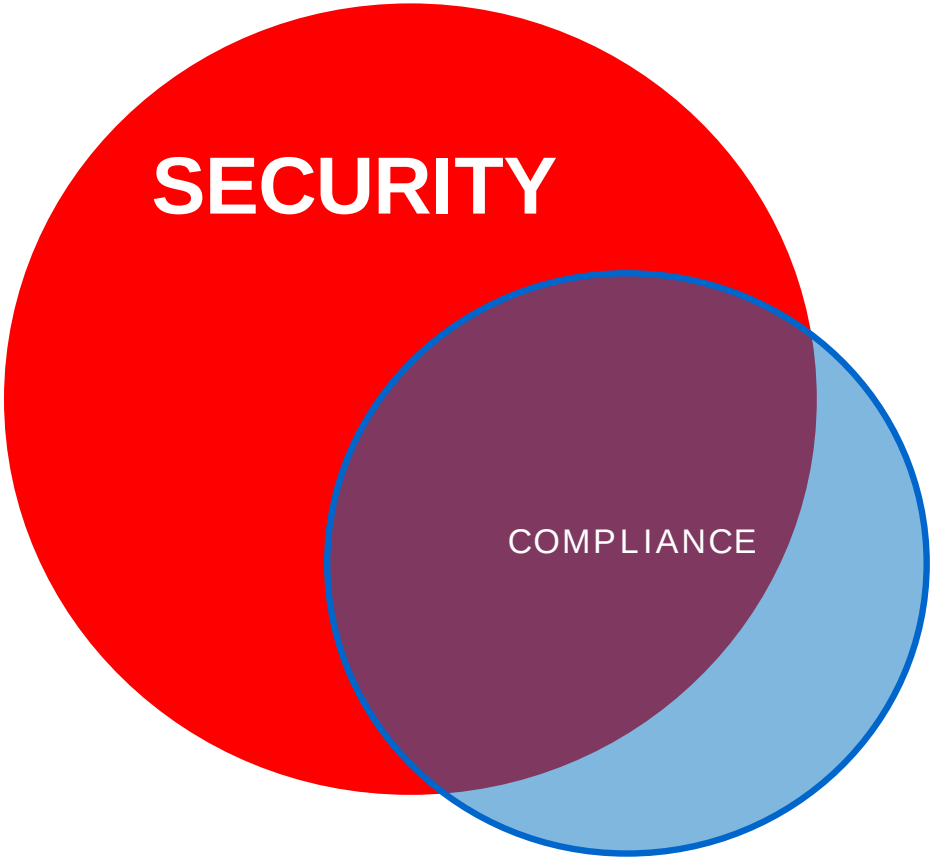


- Audit in 2014: 36 Violations

Overarching Root Causes

- Disassociation of Compliance from Security
- Business Unit Silos
- Lack of Awareness

Disassociation



Disassociation

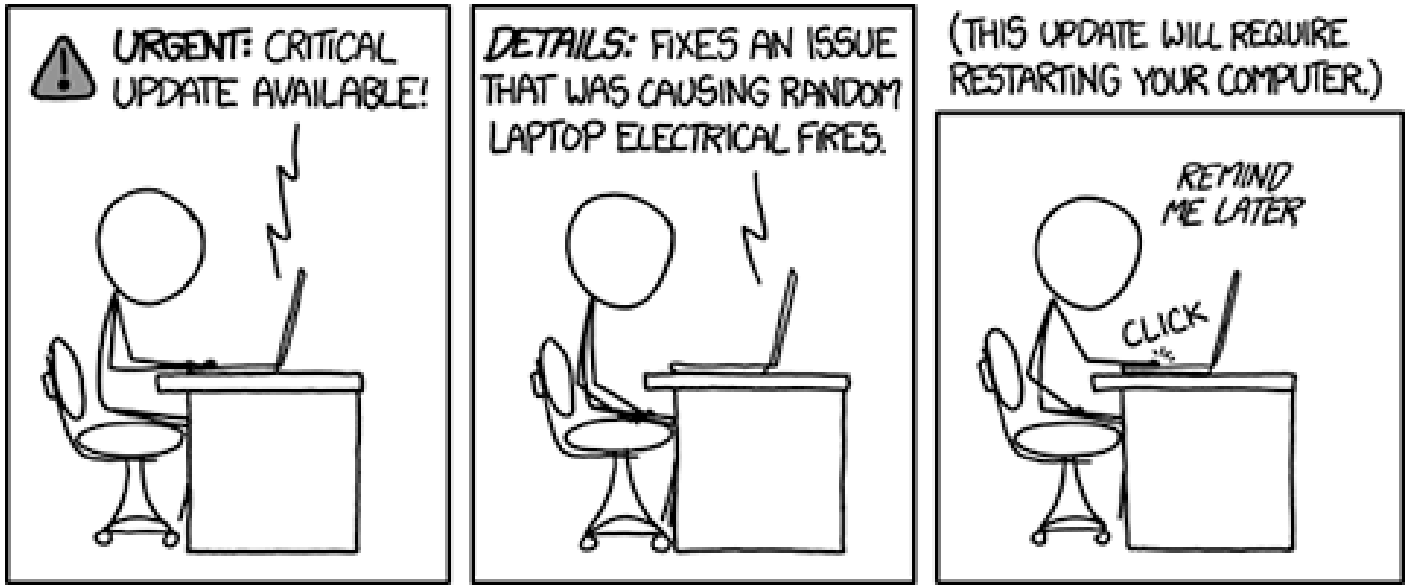
➢ Physical Security

- Manipulated three Physical Security Perimeter doors to prevent locking and ease access
- Did not prevent employee with revoked access from gaining access to control room to work eight separate shifts

Disassociation

➢ Patch Management

- Did not patch its Energy Management System after completing mitigation for same violation from 2011 compliance audit



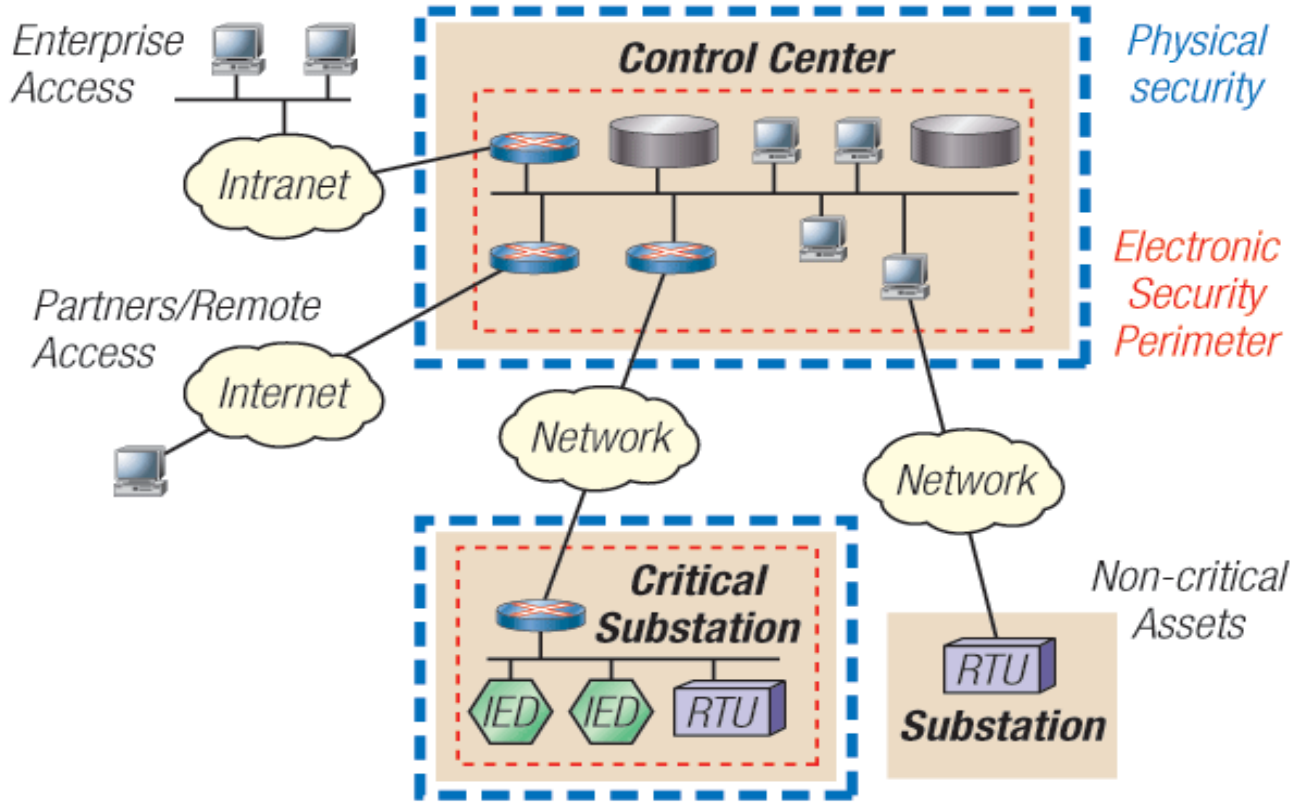
Lack of Awareness

Lack of Awareness

- **Understanding CIP Environment**

Figure 1

Electronic Security Perimeter vs. Physical Security



Business Unit Silos

Business Unit Silos

- **Workforce Management**
  - Contractors and service vendors lacked training and Personnel Risk Assessments

East Power's Response to Audit

➢ Mitigation Plan Submission

- Delay
- Baseline Mitigation
- Mitigation Disregarding Reliability

➢ Mitigation Plan Completion

- Struggled to demonstrate performance
- Late to complete mitigation
- Failure to complete four mitigation plans

RF's Redirection and East Power's Response

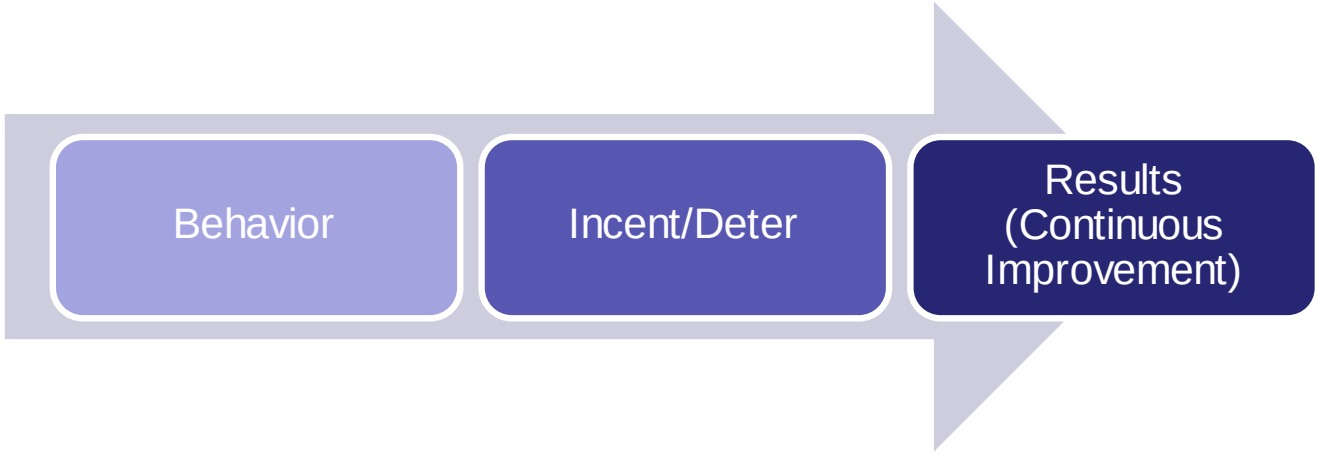
- **RF Leadership Intervention**
  - RF President meets with East Power's President and explains RF's perception of East Power and its state of cyber security

- **East Power Commits to Improve**
  - Will holistically evaluate and improve CIP compliance program

- **East Power Begins to Improve**
  - East Power creates and begins executing project plan to address overarching issues will goal of becoming best in class.

Enforcement Philosophy

- **Message**
  - Focus on reliability through a commitment to continuous improvement, strong management practices, and effective compliance programs
- **Actions**
  - Incent desired behavior (Penalty offsets, Processing treatment)
  - Deter undesired behavior (Monetary penalties, sanctions)



RELIABILITY FIRST

Opportunities for Improvement

David Sopata, Senior Reliability Consultant

Overview

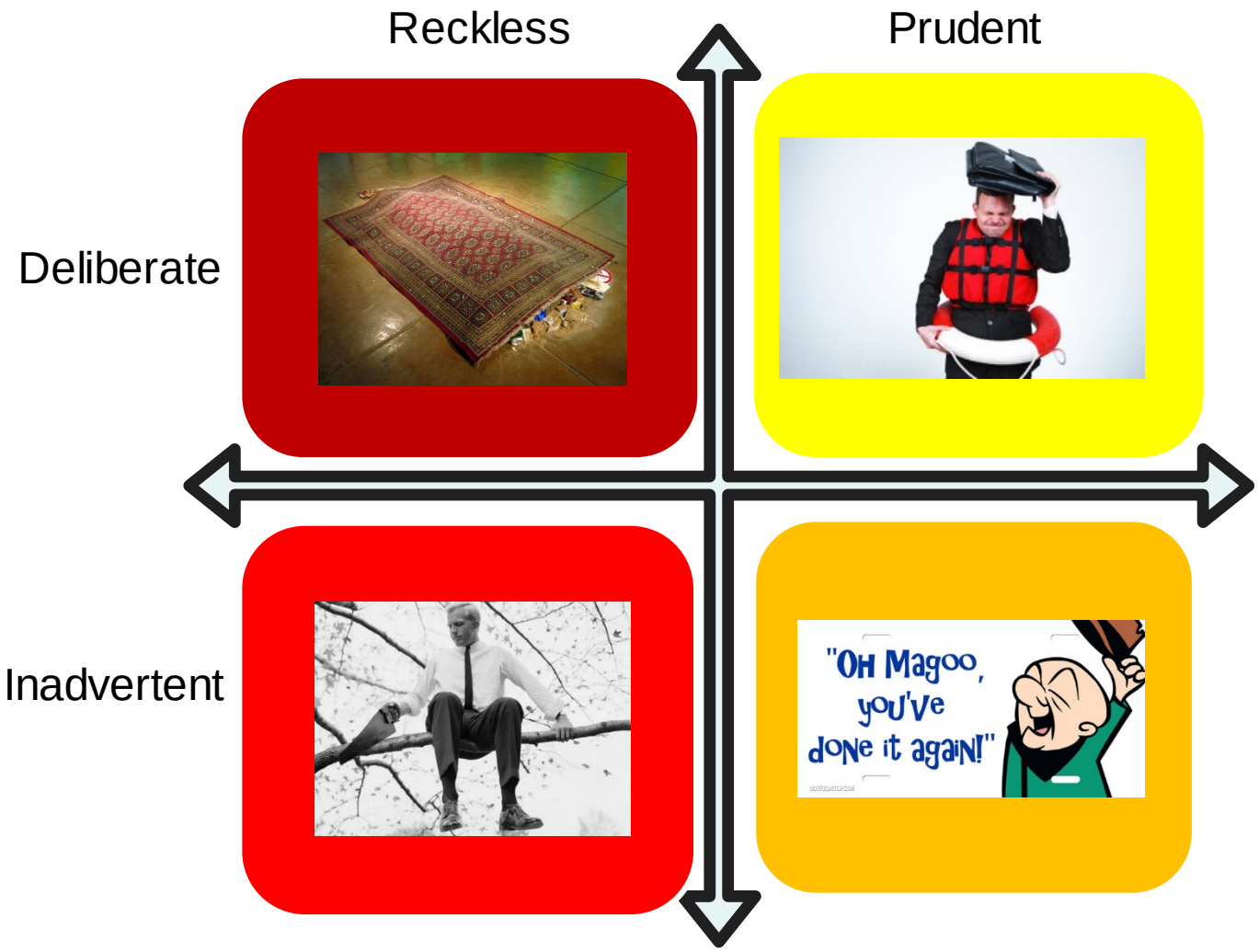
- How did East Power get to this point?
- How did East Power respond?
- What is East Power doing now?

Terminology

- **Debt**:
  - an amount of money that you owe to a person, bank, company, etc.
  - the state of owing money to someone or something
  - the fact that you have been influenced or helped by someone or something (Merriam Webster)

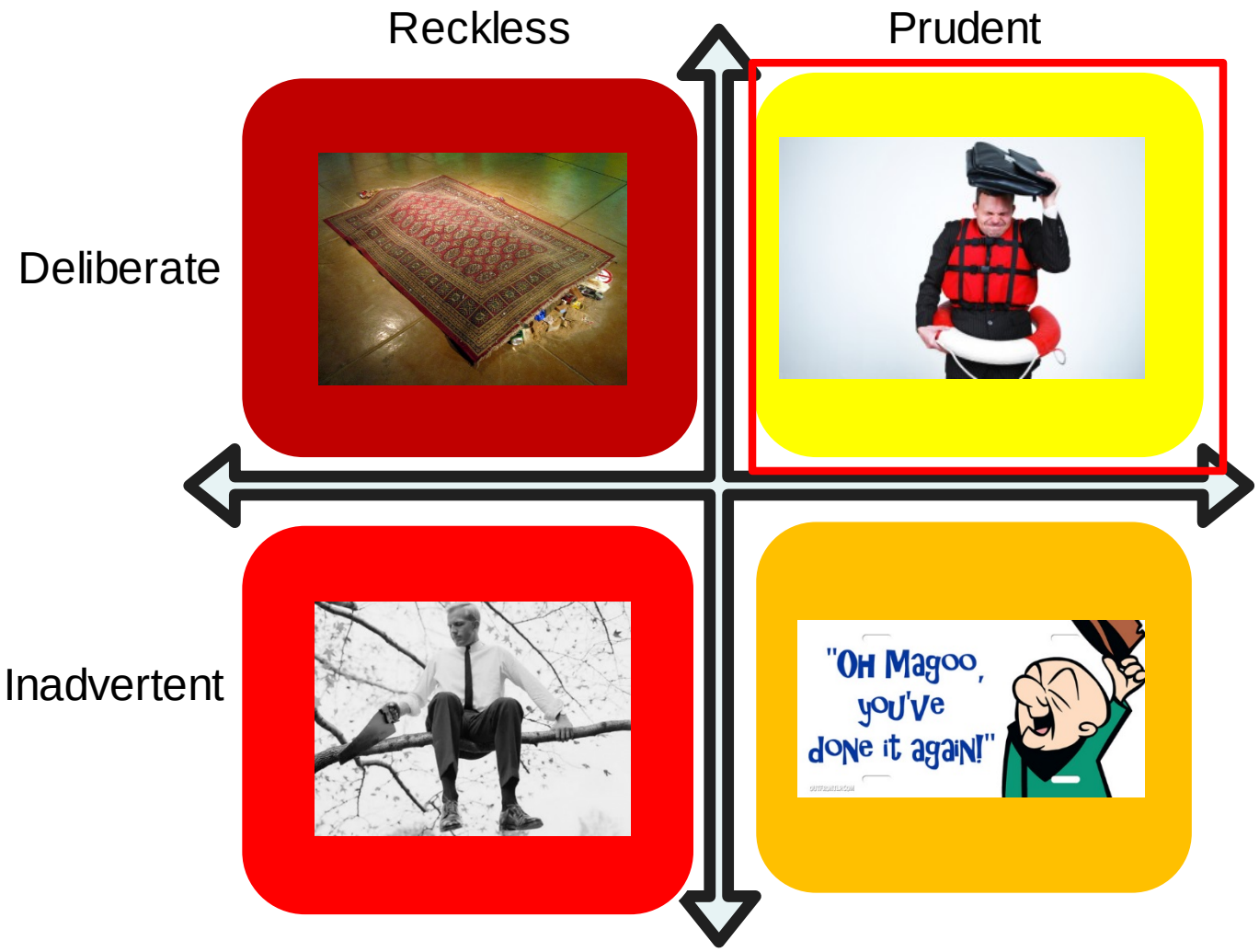
- **Technical Debt**: a metaphor coined by Ward Cunningham to explain the refactoring of software code.
  - http://agile.dzone.com/articles/understand-high-cost-technical

Technical/Compliance/Security Debt Quadrant



http://martinfowler.com/bliki/TechnicalDebtQuadrant.html

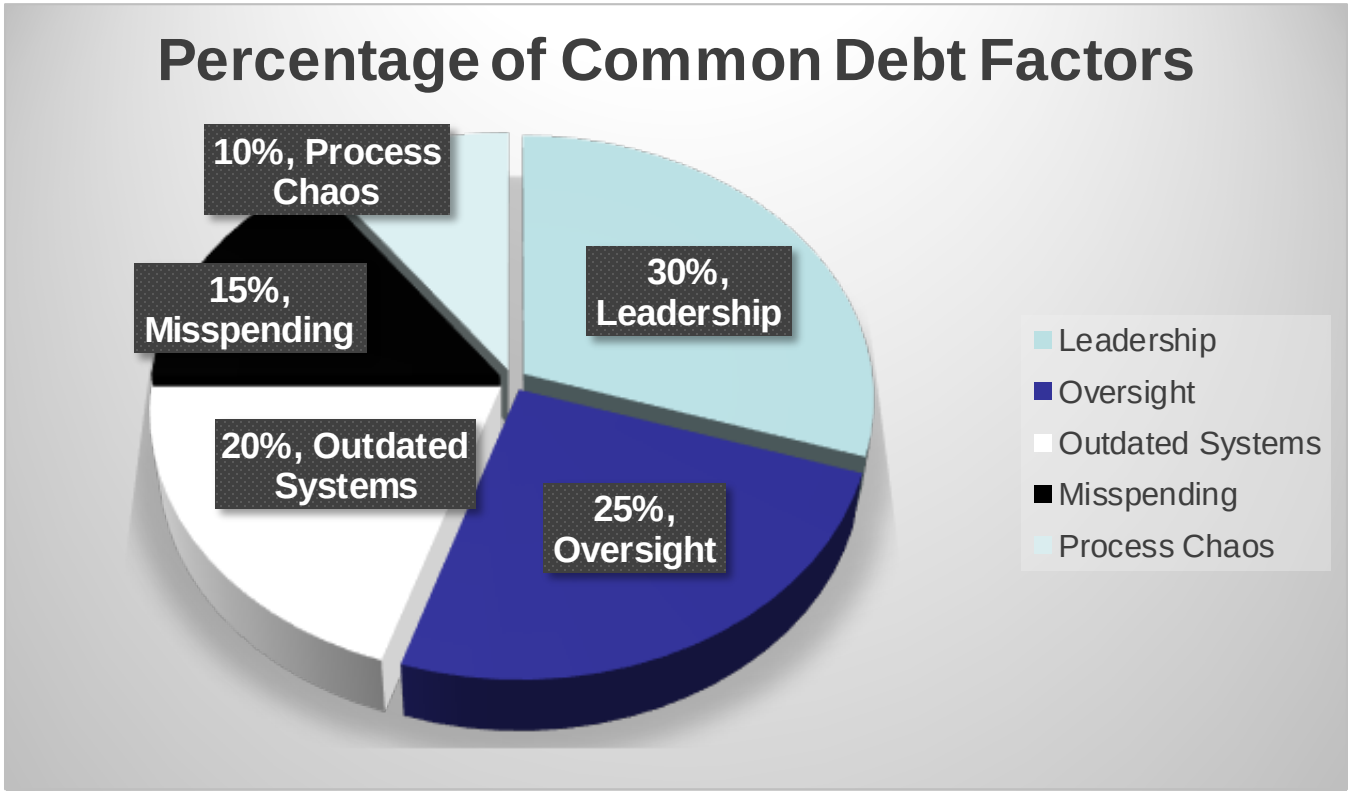
Technical/Compliance/Security Debt Quadrant



http://martinfowler.com/bliki/TechnicalDebtQuadrant.html

Technical/Security/Compliance Debt

- **What are the factors that contribute to Technical/Compliance/Security debt?**

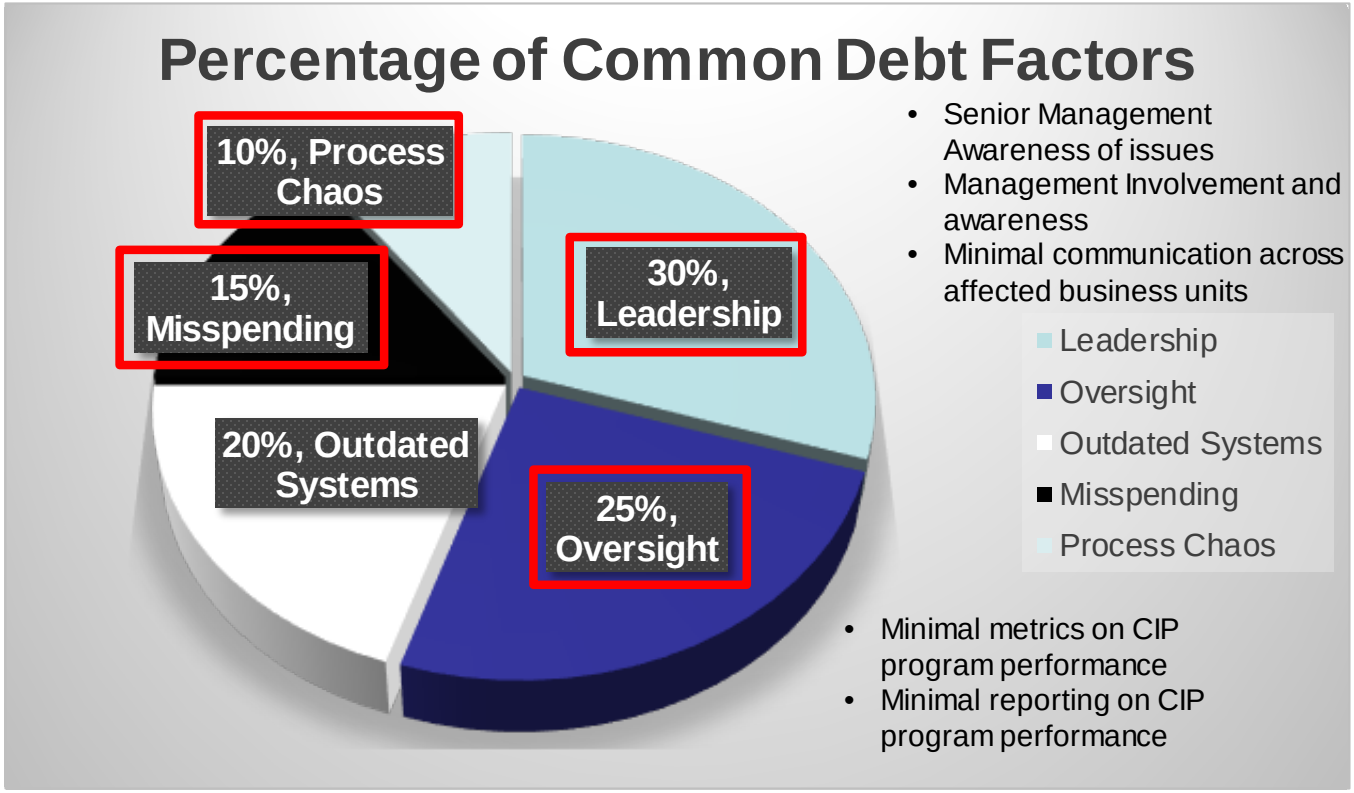


http://ww2.cfo.com/it-value/2015/05/scorecard-technology-debt/

What about East Power?

- Awareness of processes
- Understanding how one process affects another

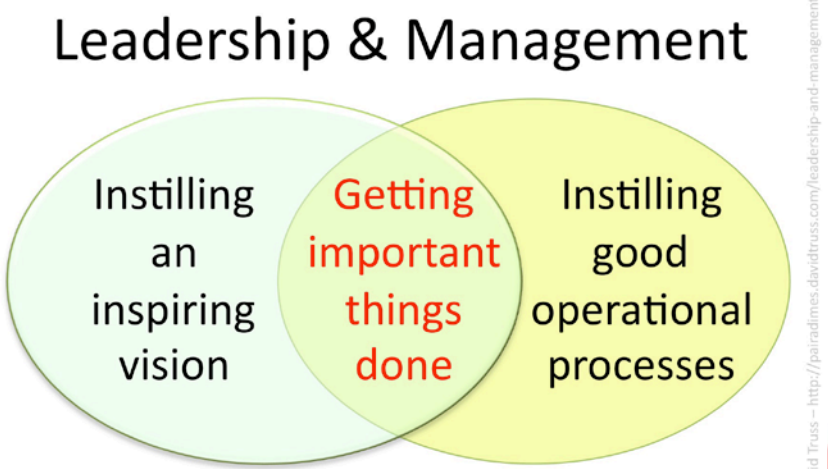
Ineffective use of:
- People
- Technology



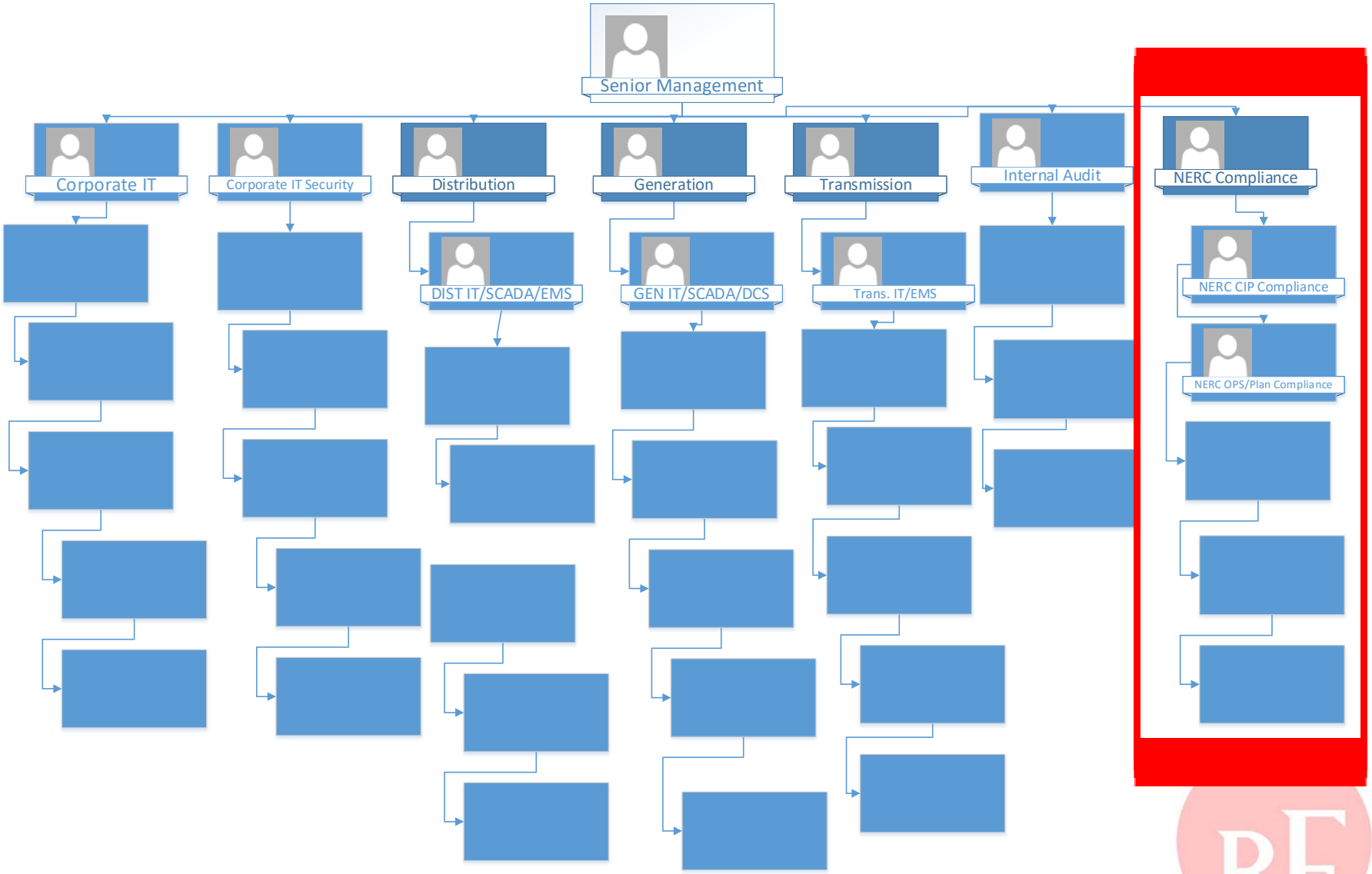
http://ww2.cfo.com/it-value/2015/05/scorecard-technology-debt/

Improved Leadership

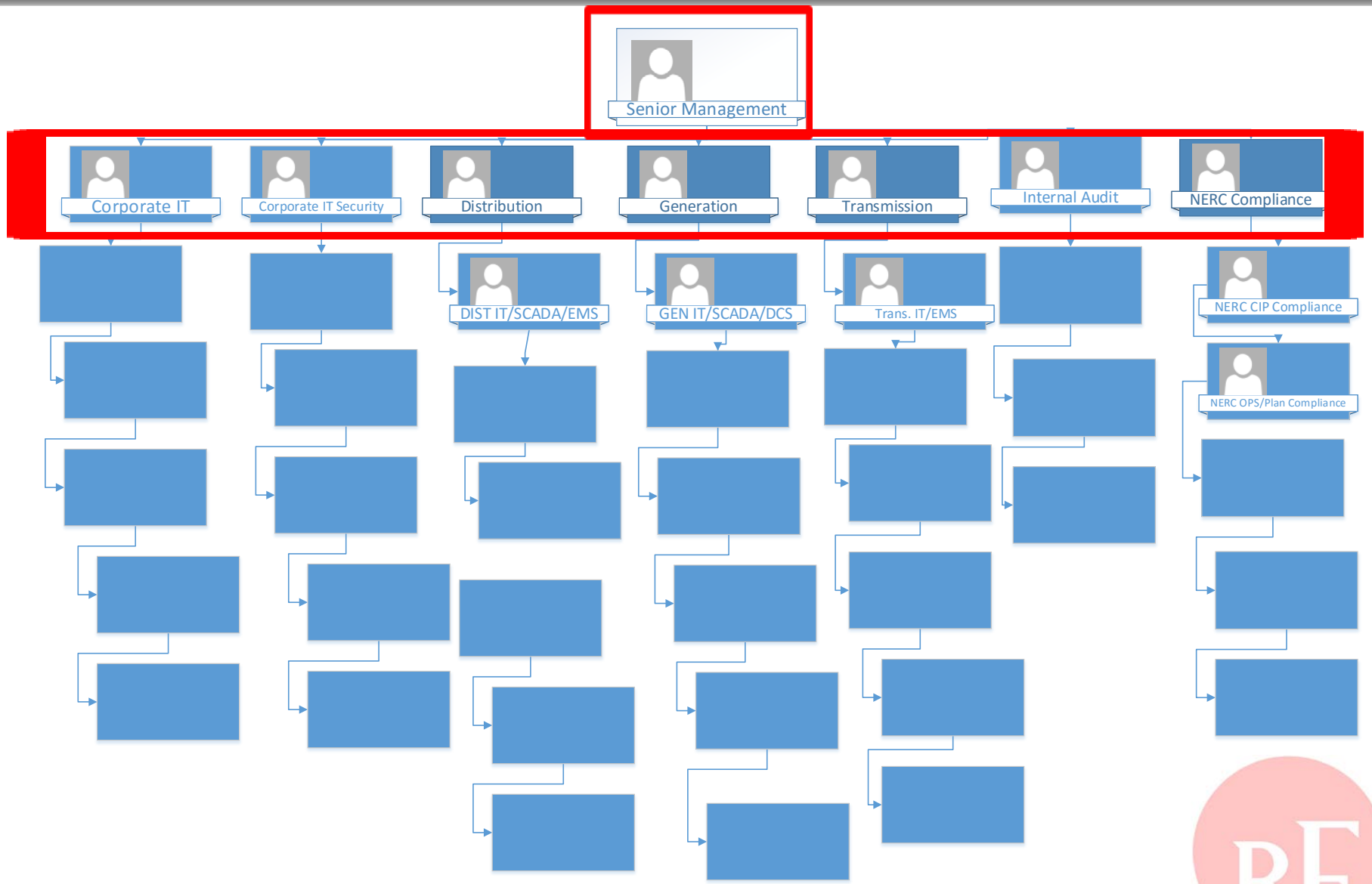
- **Compliance and continuous improvement was made a high priority, holding management and their teams accountable. This message was communicated in many ways to ensure that it permeated from top-down and across the organization.**
- **This message also required a drastic and quick cultural change within the organization that was also facilitated by senior leadership and management.**



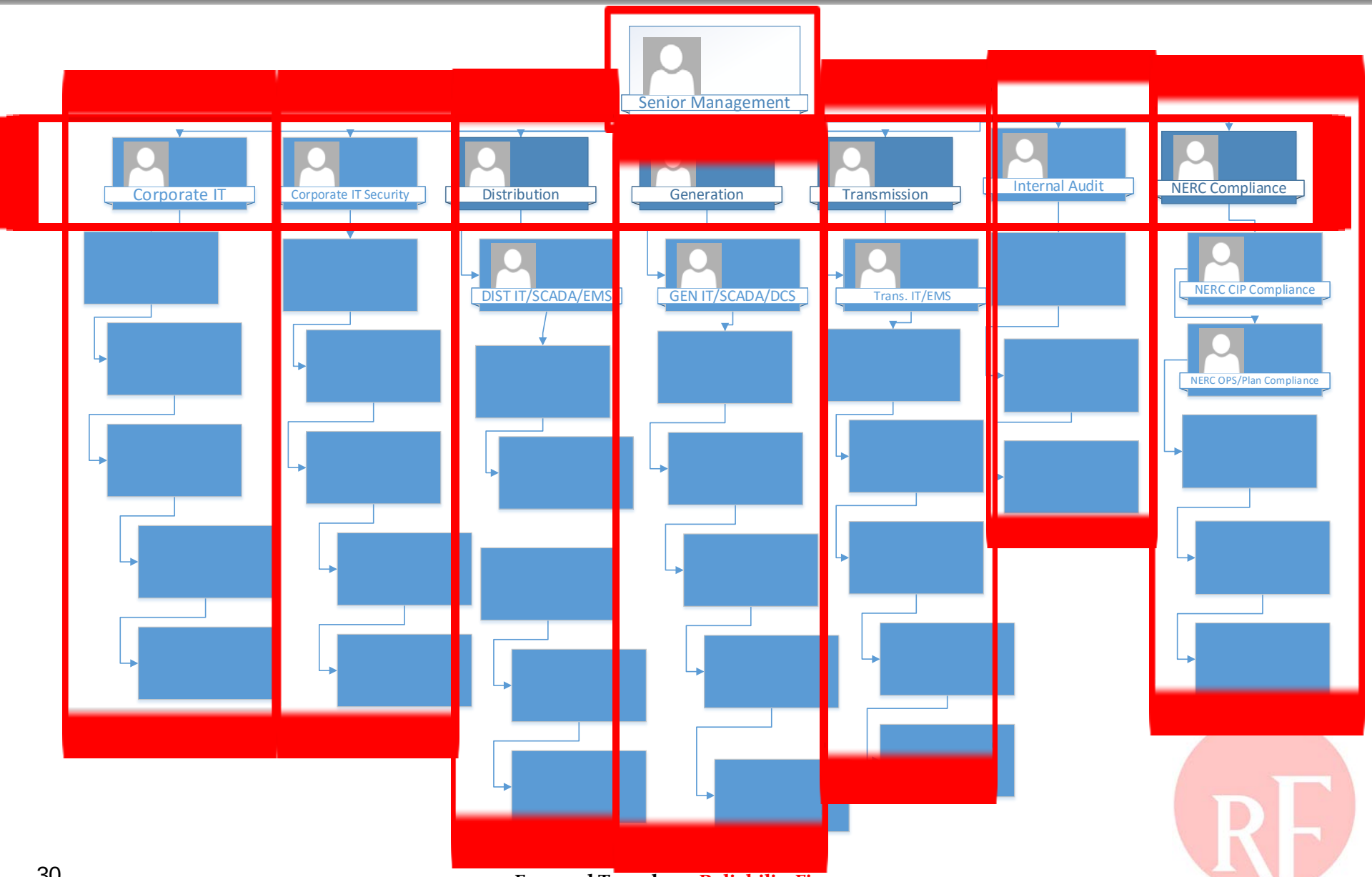
First Phase of Organizational Message



Second Phase of Organizational Message



Third Phase of Organizational Message



Increased Leadership Engagement

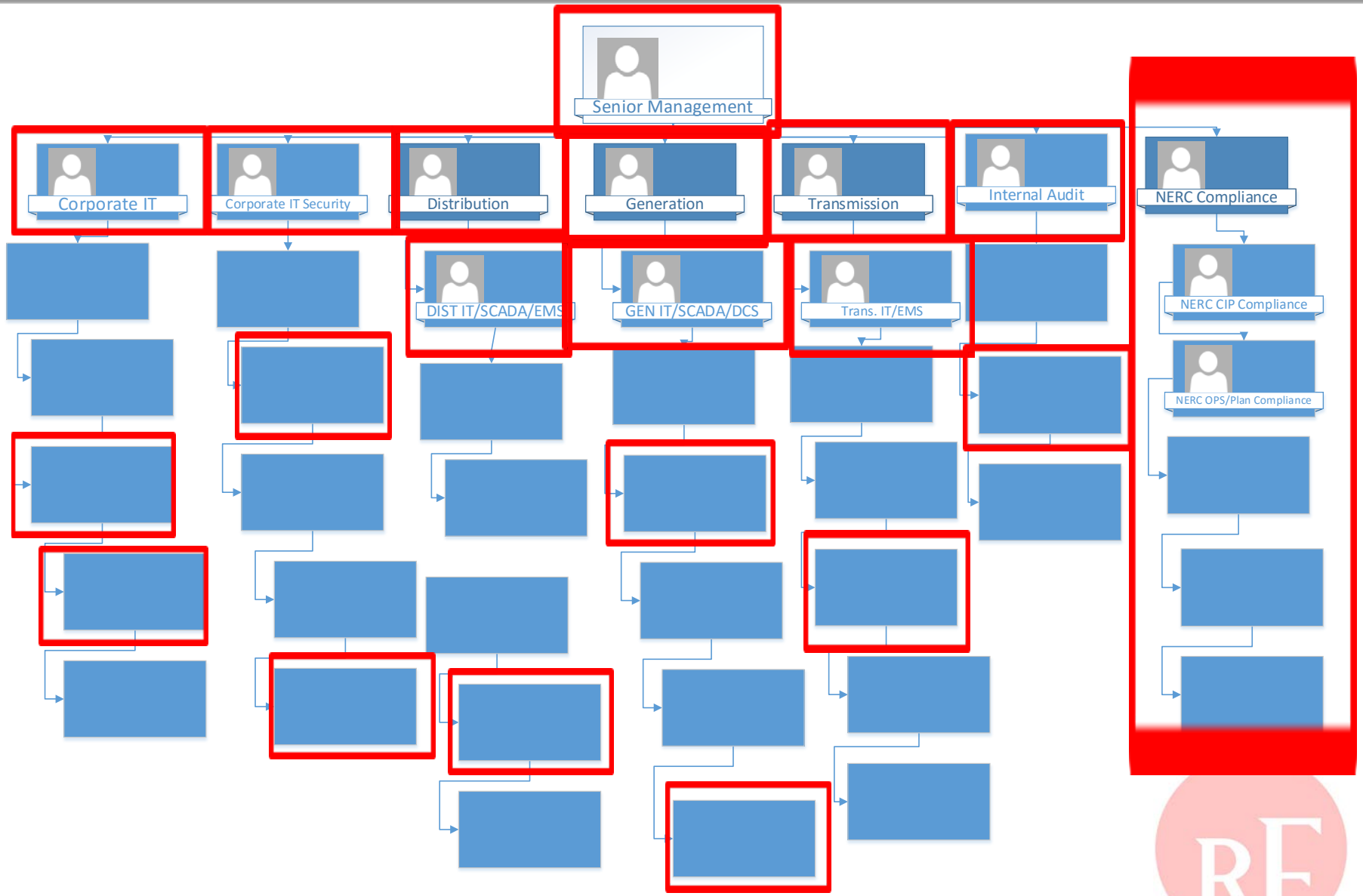
- **Description of New Culture**
  - Increased individual awareness, responsibility, and accountability regarding security and compliance for management and subject matter experts
  - Developed the ability for individual openness to report issues and mistakes to management
- **This did not happen over night!**
  - This message was communicated through multiple weeks of Senior Management meetings and team meetings.
  - The message was also continuously communicated throughout the improvement project.

Address Misspending (People)

➢ Reorganization of Compliance Department

- Brought business units representatives into compliance department and have dedicated individuals within each department to focus on compliance.
- Changed structure of group to have more individuals/managers (who directly report to the director of NERC Compliance) with designated areas of focus
- Added a continuous improvement expert (focus on improvement and root cause).
- Brought everyone into one workspace to help foster more effective and direct communication with subject matter experts.

New Team for NERC CIP Compliance



Address Misspending (People)

- **Performed a detailed analysis to understand and re-allocate roles and responsibilities**

  - ✓ Hired additional support staff and consultants
  - ✓ Dedicated teams to focus on control development and control effectiveness
  - ✓ Invested in people and resources to ensure longevity of the compliance program after remediation efforts!!!!

Address Misspending (Technology)

- ✓ Investment in new systems to help automate and monitor the systems and processes to maintain the compliance program.
- ✓ Development and implementation of new baselines for systems

Improved Oversight

- **Multi-level reports and dashboards were created to help track progress in closing program gaps**

  - Tracking policy and procedures development progress
  - Implementation tasks and priorities progress
  - Tracking potential issues and roadblocks in preventing tasks from being completed on time

Address Process Chaos

- **Dedicated teams to focus on control development and control effectiveness**
- **Dedicated team for developing and implementing new training on new systems, processes and controls**

Summary

- **East Power was able to completely turn around its security posture and improve its compliance program by:**
  - **<u>Improving the culture</u>**
    - Senior Management sending a positive message to Management and Staff that Security and Compliance are a priority
    - Senior Management and Management applying resources, people, and technology to help improve the program
    - Empowering staff to report issues or mistakes so issues can be resolved and solutions can be developed.
    - Management rewarding and showing sincere appreciation of good work and performance.

Summary

- **Fostering communication between different departments**
  - Enabling different departments to:
    - Share processes, data, and ideas
    - Collaborate on security controls and best practices
    - Share technology and tasks to improve security and compliance for corporate IT, Security, Compliance, and Energy Departments.
- **Creating Project Plans and roadmaps to:**
  - Track the progress of over **300 significant tasks over the course of 6 months** to implement a **whole CIPv5 program**!
  - Identify barriers and issues to remove and/or resolve them.
  - Improved their Self Reporting and Mitigation processes to reduce time between violation and mitigation efforts
- **Performing regular assessments with compliance, internal audit, and assist visits with Entity Development.**

Conclusion

- East Power is on track for CIPv5 by July 1st.
- They are using the extra time given by the FERC order to perform more assessments, improve their processes and procedures, and to implement more automation.
- In addition to improving processes and procedures, East Power is also striving for continuous improvement and to go above compliance for their Security program.

Questions & Answers

Forward Together **ReliabilityFirst**