



# MetricStream

EnergySec Partnered Webinar with MetricStream

Transitioning to NERC CIP Version 5: What Does it  
Mean for Electric Utilities

JANUARY 28, 2015

# Housekeeping Items



- Submit questions using control panel
- Contact information at the end for additional questions



X	Question	Asker

Send Privately   Send to All

Chat



# Panelists



**Karl Perman is a skilled business executive with 30 years of business protection, compliance, risk management, human resources and law enforcement experience. He has created, evaluated and implemented NERC reliability and critical infrastructure protection compliance programs for electric generation and transmission entities.**



**Steven Parker's experience includes more than a decade of full-time security work at critical infrastructure organizations including the Western Electricity Coordinating Council, PacifiCorp, and US Bank. He has contributed to a broad range of security projects covering areas such as e-commerce, identity management, intrusion detection, forensics, and security event monitoring.**



## MetricStream

**Mr. Schmutzler is a Regional VP for GRC solutions with a broad background including governance, risk and compliance (GRC), IT audit, risk and controls assessment, information systems design and implementation. Prior to joining MetricStream he was a Partner with KPMG LLP in the Risk Advisory Practice focused on GRC, risk assessment and systems implementation.**



# Agenda



- Effective Dates
- Cyber Assets/ BES Cyber Assets
- Structural Changes
- Bright Lines and Asset Categorization
- Evidence
- Approaches
- Automation
- Compliance Management Framework



# Effective Dates



- April 1, 2016 for high and medium systems
- April 1, 2017 for low impact systems
- Areas of Concern
  - Do not wait/Start now
  - Changing requirements (V6, V7)
  - Develop a plan including people/process/technology





# **CYBER ASSETS/ BES CYBER ASSETS/ BES CYBER SYSTEMS**



# Cyber Assets



Programmable electronic devices, including the hardware, software, and data in those devices.

- Communication networks have been removed from the definition of Cyber Asset



# BES Cyber Assets



A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)





# BES Cyber Systems



One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity



# Retired Terms



- Critical Asset
- Critical Cyber Asset





# STRUCTURAL CHANGES



# Table Based Requirements



- Applicable Systems
  - Lists device categories in-scope for requirement
- Requirements
  - Lists what must be done or accomplished
- Measures
  - Lists examples of compliance evidence
- Tables exist for requirements in CIP-004 through CIP-011



# Guideline and Technical Basis



- Provides substantial narrative discussion on the requirements
- Provides the SDT's intent for certain requirements
- Provides the technical basis for certain requirements
- Contains some conflicting or unsupported statements
- Legal status is uncertain





# BRIGHT LINES AND ASSET CATEGORIZATION



# Asset Categorization



- Bright Lines vs. RBAM
  - CIP-002 Attachment 1
  - Facilities and BES Cyber Systems
- Impact levels vs. CCA
  - High
  - Medium (ERC)
  - Low



# Asset Categorization



- All BES Facilities should be included in the application of the Impact Rating Criteria.
- All Cyber Assets located at or associated with any BES Facility should be evaluated for possible identification as a BES Cyber Asset
- BES Cyber Assets need to be logically grouped into BES Cyber Systems





# Areas of Concern



- Identification of all Cyber Assets
  - Asset management system
  - Physical walk downs
- Categorization of BES Cyber Assets
  - Stakeholder engagement
- Logical grouping of BES Cyber Assets into BES Cyber Systems
  - Approach should align with environment





# EVIDENCE



# Evidence



- Evidence is a collection of artifacts that demonstrate your compliance with the underlying requirements
  - program documentation,
  - system logs,
  - email records,
  - interviews,
  - database records, and
  - many other items.
- Consider items listed in Measures Section of Standards



# Approaches



## Manual

- Cumbersome & countless spreadsheets
- Time consuming
- Prone to errors
- Drain on resources
- Inconsistent quality
- Difficulty in reporting

## Automated

- One system- control point
- Saves time
- Reduces errors
- Reduces resource requirements
- Consistent and repeatable
- Real time reports



# Automation



- Automation aligns with several of the standards
  - CIP-002: Asset Management (Inventory)
  - CIP-004: Tying different systems into an integrated portal (HRIS, Learning, Logical Access, Physical Access)
  - CIP-007: Ports and Services and Patch Management
  - CIP-010: Change Configuration Management and Vulnerability Assessments



# Compliance Management Framework



- Does your framework?
  - Support a uniform methodology (PM)
  - Embrace collaboration
  - Integrate methodologies and processes
  - Facilitate continuous monitoring and assessment
  - Establish clear accountability/leadership
  - Foster a culture of compliance



# Thank You!







# The Role of Automation in Complying with New Standards

---



**Timothy Schmutzler**  
Regional VP of GRC Solutions  
MetricStream

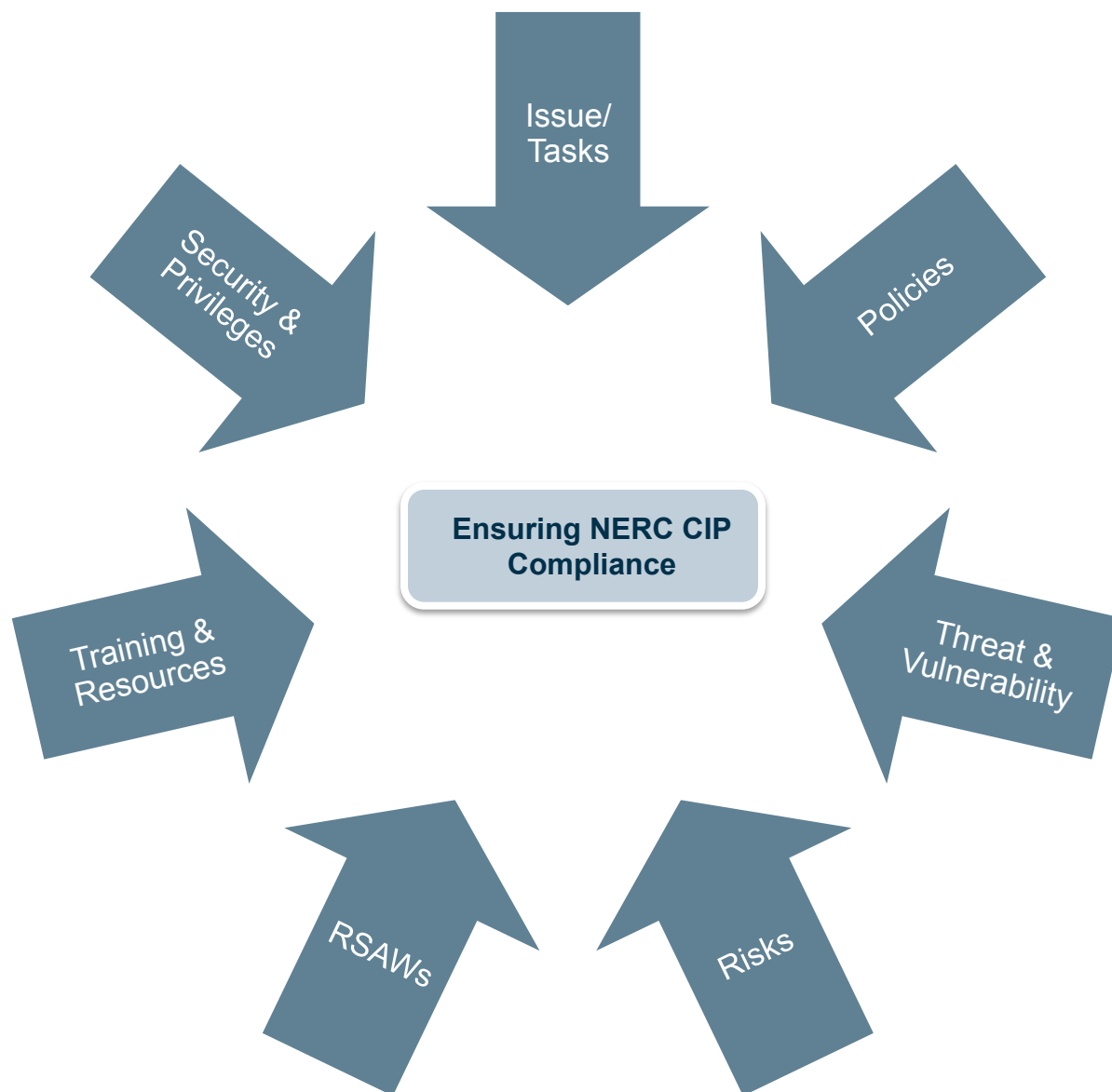


# Agenda

---

- Best Approaches to implement transition programs for NERC CIP version 5 compliance
- Advantages of having a NERC CIP Compliance Management Framework
- The role of automation in complying with new standards
- Q&A

# NERC CIP Compliance Management



# Comparing Approaches for NERC CIP Compliance

---

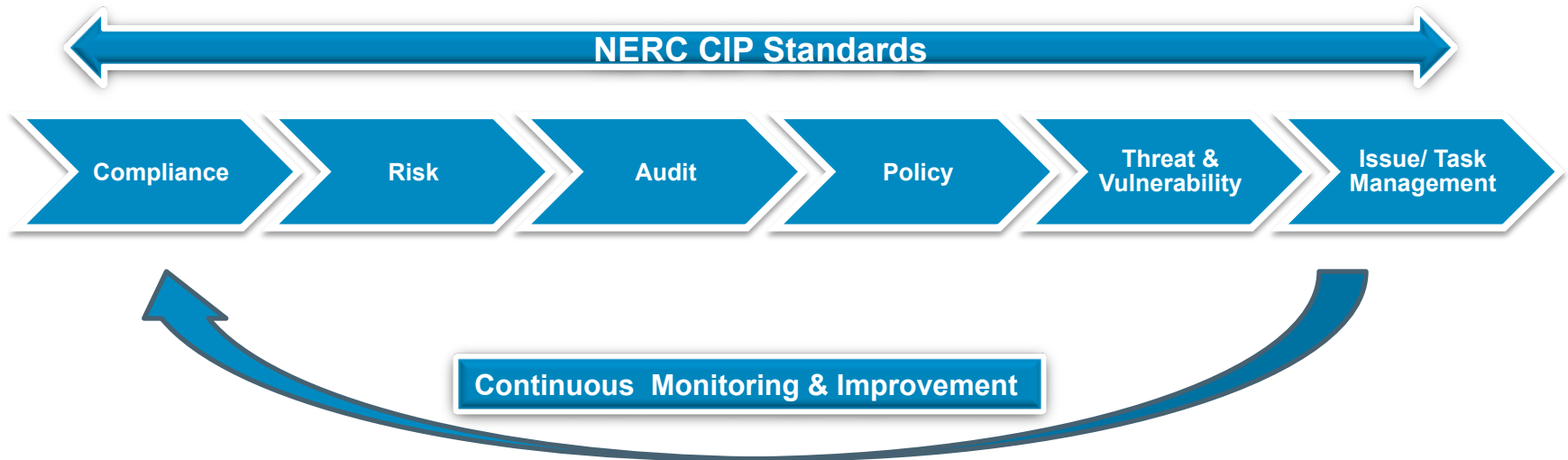
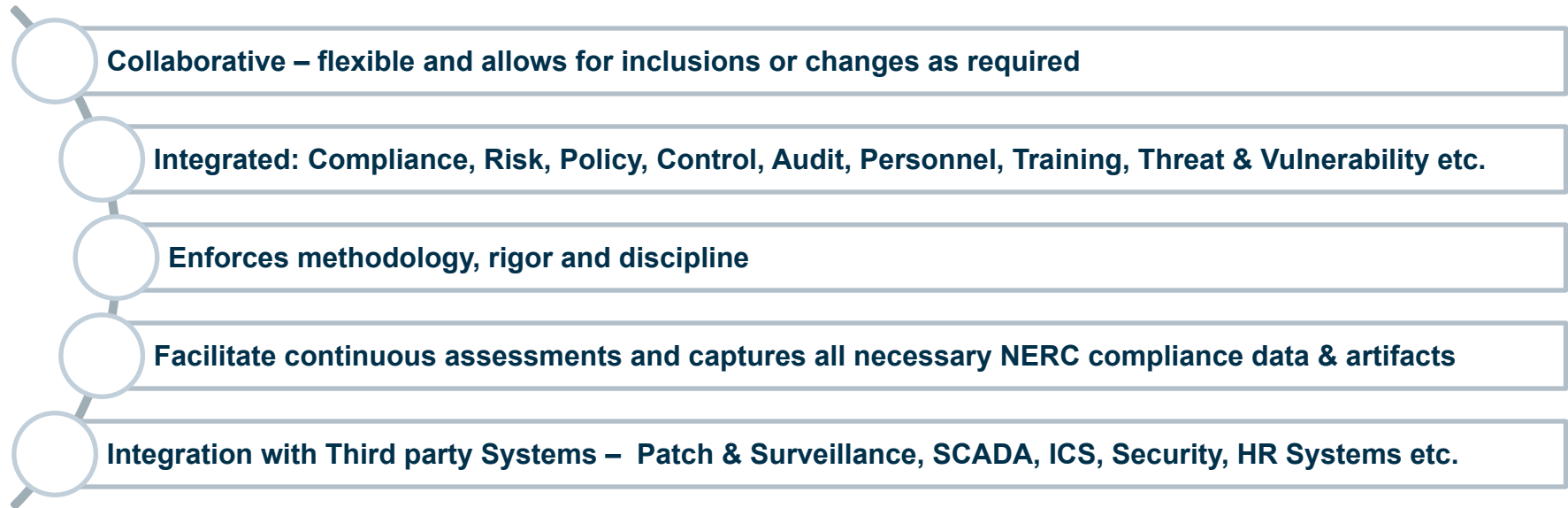
## **Traditional Approaches**

- Manual or Spreadsheets
- Time consuming; RSAW production – up to 2000hrs
- Error prone
- More resources used
- Difficult to track changes
- Tough to manage records
- Limited Reports & generation takes time

## **Automated System**

- Automated system
- Click of a button; RSAW generation is automated
- Reduction in errors
- Reduced resource needs
- Change controls in place
- Audit trail convenience
- Real time reporting with slice and dice capability

# Effective NERC - CIP Compliance Program



# Automate Compliance Assessment & Management

## Regulatory Alerts, Map Standards & Requirements

Start

## Issues and Remediation

## Regulatory Documentation

Showing 1 - 10 of 1220 records

Document	Requirements	Status	Control Count	Reference Count	Reference Description
Compliance Area 100C					
Function Name Communications					
References (e.g. Standards) COM-001-1					
Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide a means to coordinate communications among the Reliability Area. This coordination shall include the ability to investigate and implement solutions to interconnection problems within the area and with other areas.					
R1: Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall provide adequate and reliable telecommunications facilities for the exchange of interconnection and operating information.	Michael Dunlap	Active	1		Telecommunications
R1.1- Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide adequate and reliable telecommunications facilities for the exchange of interconnection and operating information.	Michael Dunlap	Active	1		Telecommunications
R1.2-Internally	Gina Horvath	Active	2		Telecommunications
R1.2-Between the Reliability Coordinator and its Transmission Operators and Balancing Authorities.	Gina Horvath	Active	2		Telecommunications
R1.3- With other Reliability Coordinators, Transmission Operators, and Balancing Authorities as necessary to maintain reliability.	Gina Horvath	Active	2		Telecommunications
References (e.g. Standards) COM-001-1					
R1.4- Where applicable, these facilities shall be redundant and diversity model.	Gina Horvath	Active	2		Telecommunications
R1.5- Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide a means to coordinate communications with other Reliability Area. This coordination shall include the ability to investigate and implement solutions to interconnection problems within the area and with other areas.	Gina Horvath	Active	2		Telecommunications

## Executive Program Management

## Compliance Assessment/ Audits

## Self-Certification, Reporting and Filing

## Reports Review & Approval

# Keep up with Regulatory Changes

The screenshot shows a web browser window displaying the MetricStream website. The browser's address bar shows the URL: [http://msdemo5.metricstream.com/soxcustom/servlets/system/Pushinfolet?id=101216&proc=3294731&user\\_asgn\\_id=120604&flag=1&CP\\_infocer](http://msdemo5.metricstream.com/soxcustom/servlets/system/Pushinfolet?id=101216&proc=3294731&user_asgn_id=120604&flag=1&CP_infocer). The website header includes a navigation bar with links like "SOX Stream", "Dashboards", "Reports", and "Documents". A search bar is present with the text "Search CO".

The main content area is titled "Interpret Alerts" and includes instructions for users. A yellow callout box labeled "Regulatory Alert Interpretation" points to a table of alerts. The table has two columns: "Select Title" and "Description". One alert is highlighted with a red circle and a red arrow pointing to the "Regulatory Alert Interpretation" box. The alert title is "FERC staff issue a Draft Environmental Impact Statement (DEIS) for the Santee Cooper Hydroelectric Project addresses the impacts of 2 hydroelectric developments in 5 counties in South Carolina (P-199-205)". The description states: "FERC staff has relicensing of the Hydroelectric Project with staff modified to adapt to the future use of Cooper rivers with protection and environmental must be filed by".

Below the table, there is a section titled "FERC" (Federal Energy Regulatory Commission) with a navigation menu including "ABOUT", "MEDIA", "DOCUMENTS & FILINGS", "INDUSTRIES", "LEGAL RESOURCES", "MARKET OVERSIGHT", "ENFORCEMENT", and "CAREERS". The "Industries" section is expanded, showing "Electric" and "Hydroelectric". The "Electric" section is further expanded, showing "Order No. 1000", "Electric Reliability", and "Smart Grid".

The "Order No. 1000" section lists several items, including "May 17, 2012 - Item E-1: FERC Denies Rehearing of Transmission Planning and Cost Allocation Rule News Release" and "July 21, 2011 - Item E-6: FERC Transmission Planning, Cost Allocation reforms to benefit consumers News Release". The "Electric Reliability" section lists "September 20, 2012 - Item E-6: FERC accepts NERC compliance filing regarding 'Find, Fix, Track Report' and provides additional time to submit additional materials Decision PDF" and "September 20, 2012 - Item E-5: FERC seeks comment on regional Reliability Standard PRC-006-NPCC-1, Automatic Underfrequency Load Shedding for the Northeast Power Coordinating Council Region News Release". The "Smart Grid" section lists "July 19, 2011 - FERC: No sufficient consensus for Smart Grid Interoperability Standards Decision PDF | NIST" and "February 16, 2011 - FERC seeks supplemental comments on Smart Grid Interoperability Standards Notice PDF | Event Details" and "December 21, 2010 - FERC staff to hold technical conference on Smart Grid Interoperability Standards on January 31, 2011 Event".

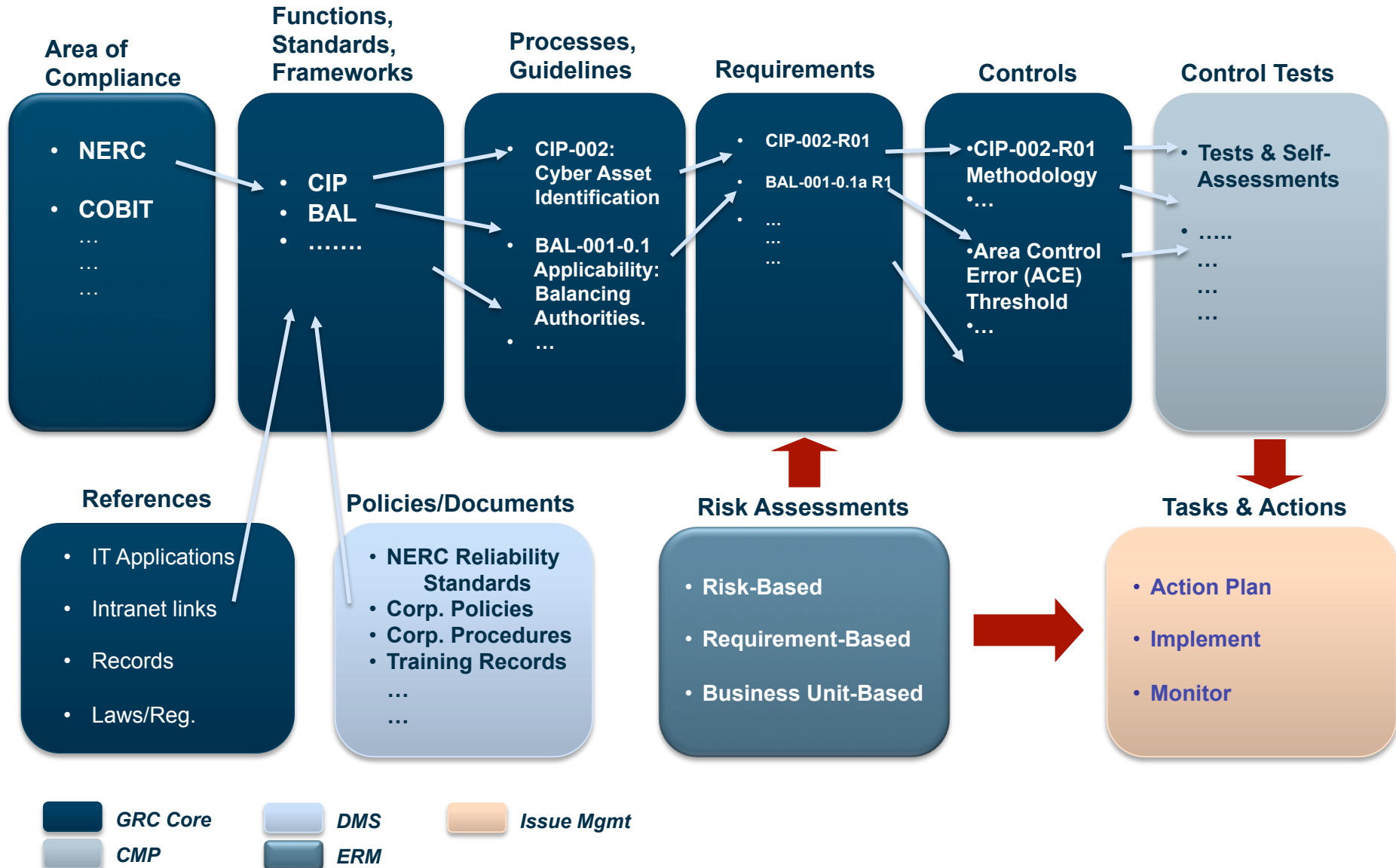
# Centralize Information Repository

- Compliance Requirements
- Risks & Controls
- BES Cyber Assets
- Threats & Vulnerabilities
- Policies & Procedures
- Personnel & Training
- Access rights and privileges
- Manage Multiple versions
- Validity dates
- ESPs, PSPs, TFEs..
- Logs & Audit Trail

The screenshot displays the MetricStream GRC Library interface. The top navigation bar includes 'Home', 'Data Upload', 'My Tasks', 'Issues', 'Compliance', 'GRC Library', and 'Administration'. The left sidebar shows a tree view of 'Browse: Areas Of Compliance' with categories like CIP-001-1, CIP-001-2a, CIP-002-3 (selected), CIP-002-4, CIP-003-3, CIP-003-4, CIP-004-1, CIP-004-3, CIP-004-4, CIP-005-1, CIP-005-4a, CIP-006-1, CIP-006-4c, CIP-007-4, CIP-008-4, CIP-009-4, and PRINCIPAL INVESTMENT ACTIVITY/. The main content area is titled 'Area Of Compliance: CIP-002-3 [AOC-1007]'. It contains a 'Name\*' field with 'CIP-002-3', a 'Regulatory Body' dropdown set to 'NERC', and a 'Version #' field with '3'. Below this are tabs for 'Details', 'Organizations', 'Related To', and 'Additional Details'. The 'Details' tab is active, showing a 'General' section with a 'Description' field containing text about CIP-002-3 requirements. The 'Ownership and Security' section includes 'Owner Organizations\*' (Corporate HQ), 'Owners' (Mike Morton), 'Level 1 Approver', 'Level 2 Approver', and 'Restrict Access To\*' (No Restriction). The 'Validity (Dates)' section shows 'Valid From' (08/01/2011) and 'Valid Until' (31). The 'Modify/Review/Approve' section has an 'Action\*' dropdown set to 'Submit' and a 'Comments' field.

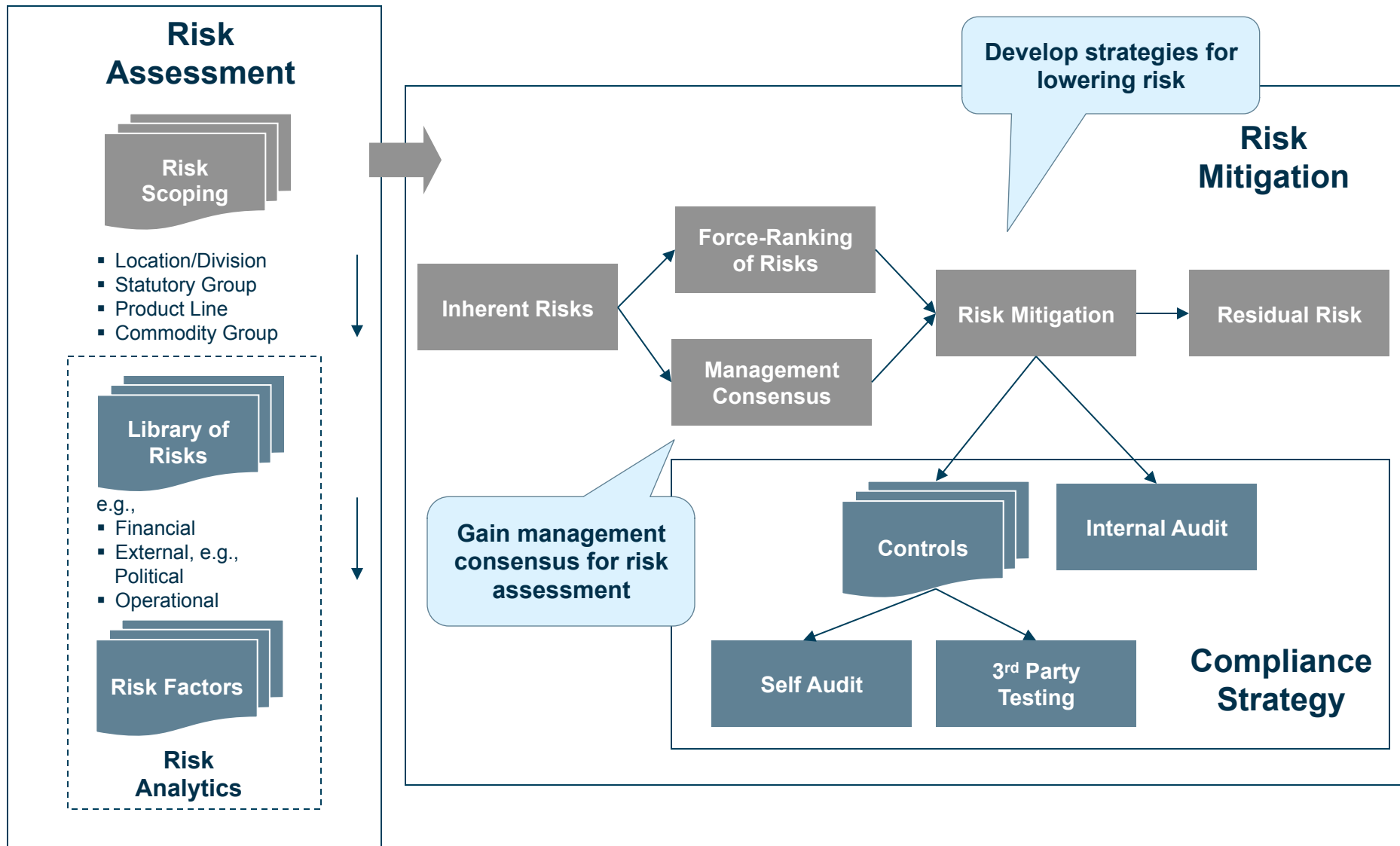
Library of Compliance Standards Mapped to Org Structure

# A Robust & Flexible Information Model





# Collaborative Risk and Compliance Management



# Facilitate BES Cyber Asset Identification

- Create or Import Asset Information
- Risk based Assessments to identify Cyber Assets
- Bright line criteria
- Threat & Vulnerability Assessments on Assets
- Impact Analysis on Assets
- Assigning Assets to specific Electronic Security Perimeters (ESPs)
- Automate Annual Review Approval

**Create Asset/System/Application**

Welcome: Scott Kinney

**MetricStream**

Compliance Center | To Dos | Dashboards | My Profile | Assignments

Home | NERC Dashboard | FERC Dashboard | My Dashboards and Reports

**Create Asset/System/Application**

Fields marked with a red asterisk are required.

**Asset Information**

Asset ID: Asset-ID-2 | Asset Type: Select One | Asset Sub-Type: Select One

Name:

Manufacturer: Select One | Model:

Status: Select One | Active Since: mo. / day / year

Comprises of Asset(s):

**MetricStream** | Welcome: MetricStream Administrator | My Tasks: 30 [20 New, 0 Past due]

GRC Library | Issues | AppStudio | My Tasks | **IT GRC** | Administration | System

Manage Compliance Program | Manage Assets | External Upload | View Executive Dashboard

**Addit >> Threat and Vulnerability Posture Report (QualysGuard)**

Report Data as of: 08/24/2011 01:45 AM

QID	Title	Vulnerability Type	Severit...	Patcha...	Category
Asset: (IP 172.18.0.6) (DNS msi-fs02.metricstream.com) (NETBIOS MSI-FS02)					
105185	Microsoft Windows Effective Permission on ...	Information Gathered	2	0	Security Policy
105316	Windows Shares With Everyone Group Hav...	Information Gathered	2	0	Security Policy
105317	Windows Shares With Everyone Group Hav...	Information Gathered	2	0	Security Policy
105335	Microsoft Windows Permission on Shares E...	Information Gathered	2	0	Security Policy
11	Hidden RPC Services	Vulnerability	2	0	RPC

Identify and Manage Assets and Asset Ratings

# Implement Cyber Security Management Controls

- Define and Manage Controls to protect Cyber Assets
- Manage Password Changes
- Perform Control Assessments on regular basis
- Control Tests to identify strength of controls
- Notifications to appropriate officers
- Logs and audit trail maintenance
- Equivalent to Self Correcting Process Improvement mentioned in Version 5

The screenshot displays two overlapping web browser windows from MetricStream. The top window shows the 'Control Self Assessment' form, which includes fields for Business Unit (Audit Division), Control Number (CT-110514), Due Date (03/16/2010), and Control Name (Any payments greater than 10k require 3 levels of approval). It also features a dropdown menu for 'Is the Control operating effectively?' with options 'Select One', 'No', and 'Yes'. The bottom window shows the 'Test Execution' form, which includes fields for Business Unit (CBO), Test Number (TP-103933-2007-00001), Test Name (Test 1.1.6.a), Test Performed By (Business Unit), and Type (Initial Testing). It also has a 'Test Plan Comments' section and a table for 'Test Execution' results.

Activity	Response	Business Unit	Activity Score*	Passed	Failed
1.1.6.a Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.		CBO	Select one...		

Implement and Assess Controls

# Integrate Personnel & Training Management into Compliance

Selecting & assigning appropriate Courses to Employees

Initiate Training

Report Course Completion

Creating Questionnaire

Administering Tests

Reports - Training Gap

Creating and Assigning Competency

Certification

**Initiate Training Request**

Fields marked with a red asterisk are required.

**Request Number** **Initiated By**  
Manager1

**Enter Details of Training Request**

**Org - Entity Level\*** Corporate **Org - Name\*** Corporate

**Training Need Type/Origin\*** Organization Need

**Department** Select One **Group** Select One

**Training Course Details**

Delete [Add Row](#) [Delete Last Row](#) Total Rows: 1

☐ **Course Name\***

**Expectation**

**Post Training Testing Required?**  
Select One

**Training Feedback Required?**  
Select One

**Comments**

**Initiator's Comments**

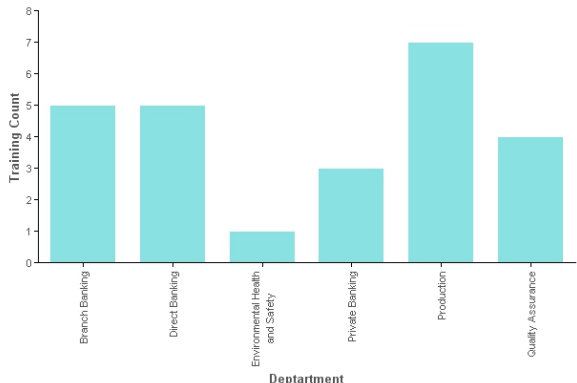
**Reports**

[Training Gap Report \(Course\)](#)

**No of Trainings per Department**

No of Trainings per Department [Show Tree]

Training Count per Dept



Department	Training Count
Branch Banking	5
Direct Banking	5
Environmental Health and Safety	1
Private Banking	3
Production	7
Quality Assurance	4

Done Refresh Create Dashboard View Assign Charts

- Personnel risk assessment, training, and security awareness
- Understanding Compliance Regulations
- Accepting and understanding organization policies
- Reports - Training Medium, Gaps, Trained-Untrained Employee Breakup

- Policies & Procedures for Implementing a physical security program
- Setting prerequisites for granting approvals, assigning work etc.
- Define methods, processes, and procedures for securing Cyber Assets & BES



# Real time Monitoring and Reporting

- Risk Intelligence by Regulations & Assets
- Track NERC version and Migration status
- Monitor NERC Compliance Audit Readiness
- Regulatory Filings, Certifications

**Risk Report**

Report Data as of: 03/07/2011 04:07 AM

mo. / day / year hrs. : mins. PM

[Create Search Condition](#)

Search Condition

Showing 1 - 8 of 8 records

Standard	Requirement Description	Version	Asset Type	Risk Category	Status
CIP 002	Critical Cyber Asset Identification	V3	Transmission SCADA	Technical	Compliant
CIP 003	Security Management Controls	V3	Distribution SCADA	Management	Non Compliant
CIP 004					
CIP 005					
CIP 006					
CIP 007					
CIP 008					
CIP 009					

Welcome: Scott Kinney

**MetricStream**

[Compliance Center](#) [To Dos](#) [Dashboards](#) [My Profile](#) [Assignments](#)

**CIP V3 Goodness Check and V4 Migration**

Report Data as of: 03/07/2011 03:58 AM

mo. / day / year hrs. : mins. PM

[Create Search Condition](#)

Search Condition

Showing 1 - 4 of 4 records

Standard	Requirement Description	V3 Status	V4	V4 migration Action Plan
<a href="#">CIP 002</a>	Critical Cyber Asset Identification	Non Compliant	Non Compliant	<a href="#">CIP 002 Cyber Security — Critical Cyber Asset Identification</a>
<a href="#">CIP 003</a>	Security Management	Compliant	Non Compliant	<a href="#">CIP 003 Cyber Security — Security</a>
<a href="#">CIP 004</a>				
<a href="#">CIP 009</a>				

**Dashboard 1 Compliance Program Status**

Note: Many test executions and issues affect more than one process and areas of compliance and as a result may be reflected multiple times in this report.

Report Data as of: 05/07/2011 05:42 AM

mo. / day / year hrs. : mins. PM

Showing 1 - 20 of 24 records

Standard Name	Requirement	Task Status (Current)			Survey Status (Year to Date)				Issue Status (Current)		
		Completed	Pending	Total Tasks	Completed	Overdue	Notdue	Total	Open Current	Open Overdue	
<b>Business Unit MSI</b>											
<b>Area of Compliance NERC</b>											
ERC-001-0.1a	2	2	0	2	0	0	0	0	0	0	
CIP-001-1	4	3	0	3	0	0	0	0	0	0	
CIP-002-1	13	9	0	9	0	0	0	0	0	0	
CIP-003-1	19	16	0	16	0	0	0	0	0	0	
CIP-004-1	13	12	0	12	0	0	0	0	0	0	
CIP-005-1	12	3	0	3	0	0	0	0	0	0	
CIP-006-1	15	2	0	2	0	0	0	0	0	0	
CIP-007-1	14	4	0	4	0	0	0	0	0	0	
CIP-008-1	8	3	0	3	0	2	0	2	2	0	
CIP-009-1	7	5	0	5	0	0	0	0	0	0	
COM-001-1	2	3	0	3	0	0	0	0	0	0	
ERP-001-0	1	1	0	1	0	0	0	0	0	0	

# MetricStream Advantage - NERC CIP Solution

---

- Best in class Governance, Risk and Compliance solutions provider
- Platform based solution – with integrated risk, compliance, policy, issue and change management systems
- Experience in working with numerous electric utilities in the US ranging from co-ops to investor owned
- Built in content with controls and industry best practices
- One-Click Automated RSAW generation – reduction in RSAW production times from weeks to just few hours/ days.
- Have real-time visibility into business to avoid compliance concerns

# About MetricStream

## Vision

Integrated Governance, Risk & Compliance (GRC) for Risk-Driven Intelligence and Better Business Performance

## Solutions

- NERC CIP Compliance
- Risk Management
- Compliance Management
- Audit Management
- Legal GRC
- Supplier Governance
- Quality Management
- EHS & Sustainability
- IT-GRC
- Governance & Ethics

## Partners



## Organization

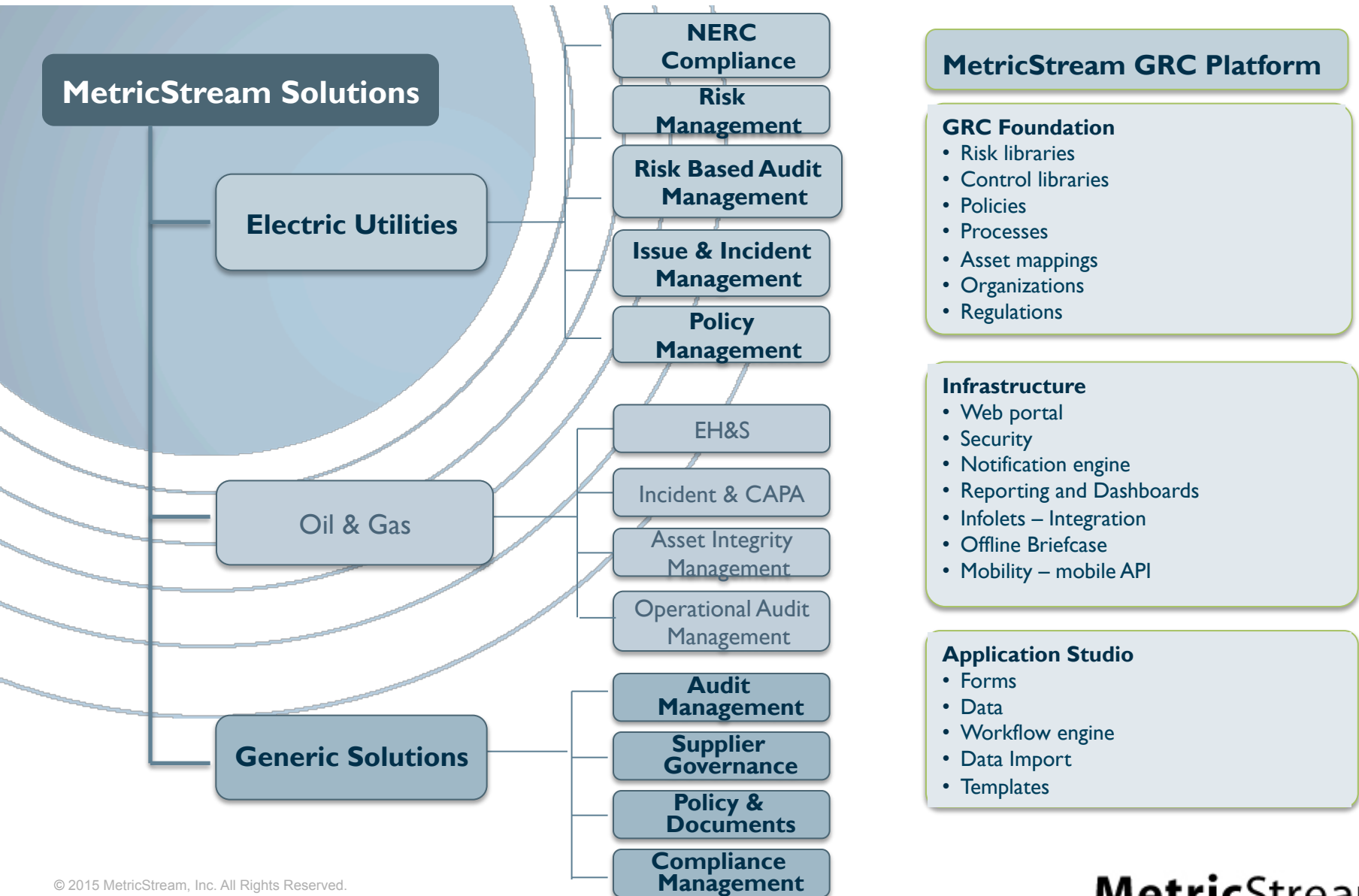
- Over 1,800+ employees
- Headquarters in Palo Alto, California with offices worldwide
- Over 335 enterprise customers
- Privately held – backed by leading global VCs

## Differentiators

- Technology - GRC Platform – 9 Patents
- Breadth of Solutions – Single Vendor for all GRC needs
- Cross-industry Best Practices and Domain Knowledge
- ComplianceOnline.com - Largest Compliance Portal on the Web



# MetricStream Solution Areas - ENU



# Q&A



**Karl Perman**

Director, Member Services  
EnergySec

Email – [karl.perman@energysec.org](mailto:karl.perman@energysec.org)



**Steven Parker**

President  
EnergySec

Email – [steven.parker@energysec.org](mailto:steven.parker@energysec.org)



**Timothy Schmutzler**

Regional VP of GRC Solutions  
MetricStream

Email - [tschmutzler@metricstream.com](mailto:tschmutzler@metricstream.com)

Please submit your questions to the host by typing into the chat box on the lower right-hand portion of your screen.

**Thank you for participating!**

A copy of this presentation will be made available to all participants in next 48 working hours.

For more details on upcoming MetricStream webinars: <http://www.metricstream.com/webinars/index.htm>

# Thank You

---

## Contact Us:

Website: [www.metricstream.com](http://www.metricstream.com) | Email: [webinar@metricstream.com](mailto:webinar@metricstream.com)

Phone: USA +1-650-620-2955 | UAE +971-5072-17139 | UK  
+44-203-318-8554



[Join us on RACE Group](#)



[Follow us on Twitter](#)



[Like us on Facebook](#)