

# Preparing for the NERC CIP Audit - Importance of Maintaining and Providing Evidence of Compliance



**Karl Perman**  
VP Member Services  
EnergySec



**Shreyank Shrinath Kamat**  
Product Manager  
MetricStream

## Agenda

---

- ⦿ Preparing for audits strategy
- ⦿ Providing timely documentation and evidence of compliance through a central repository of evidence
- ⦿ Robust process and best practices to document audit reports for compliance program
- ⦿ Knowledge management: Documenting subject matter expert's discussions and decisions
- ⦿ Q&A

# Preparing for the NERC CIP Audit



**Karl Perman**  
VP Member Services  
EnergySec



# Definitions

**Documentation:** the act or an instance of furnishing or authenticating with documents  
the provision of documents in substantiation

**Evidence:** something which shows that something else exists or is true  
a visible sign of something  
material that is presented to a court of law to help find the truth about something

Source: Merriam Webster OnLine



# Documentation Examples



- BES Cyber System Identification
- Cybersecurity Policies
- Security Awareness
- Security Training
- Personnel Risk Assessment
- Access Management
- Electronic Security Perimeters
- Physical Security Plan
- Patch Management
- Malicious Code Management
- Incident Response
- System Recovery
- Configuration Management
- Vulnerability Assessments
- Information Protection



# Evidence Examples



- Written documentation
- Performance evidence
- Verbal testimony
- Communication records
- Observations





# Evidence Tips

- Know where to find evidence
- Evaluate evidence independently
- Balance the details; auditors will request additional information if necessary
- Redact where appropriate (sensitive information)
- Common format-use the RSAW and build a substantive and clear narration
- Be mindful of BCSI and your IPP
- Be prepared to “prove it”- the burden is on you to demonstrate compliance



# Audits



- Audits are about:
  - Accountability
  - Transparency
  - Consistency
  - Sustainability
- Compliance Framework
- Audit etiquette



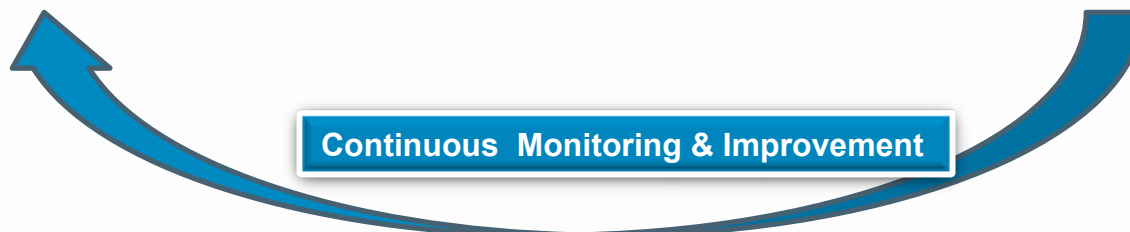
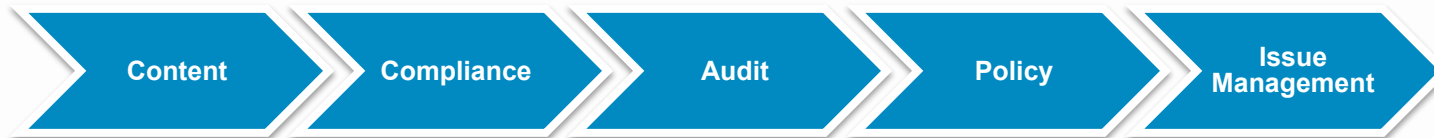
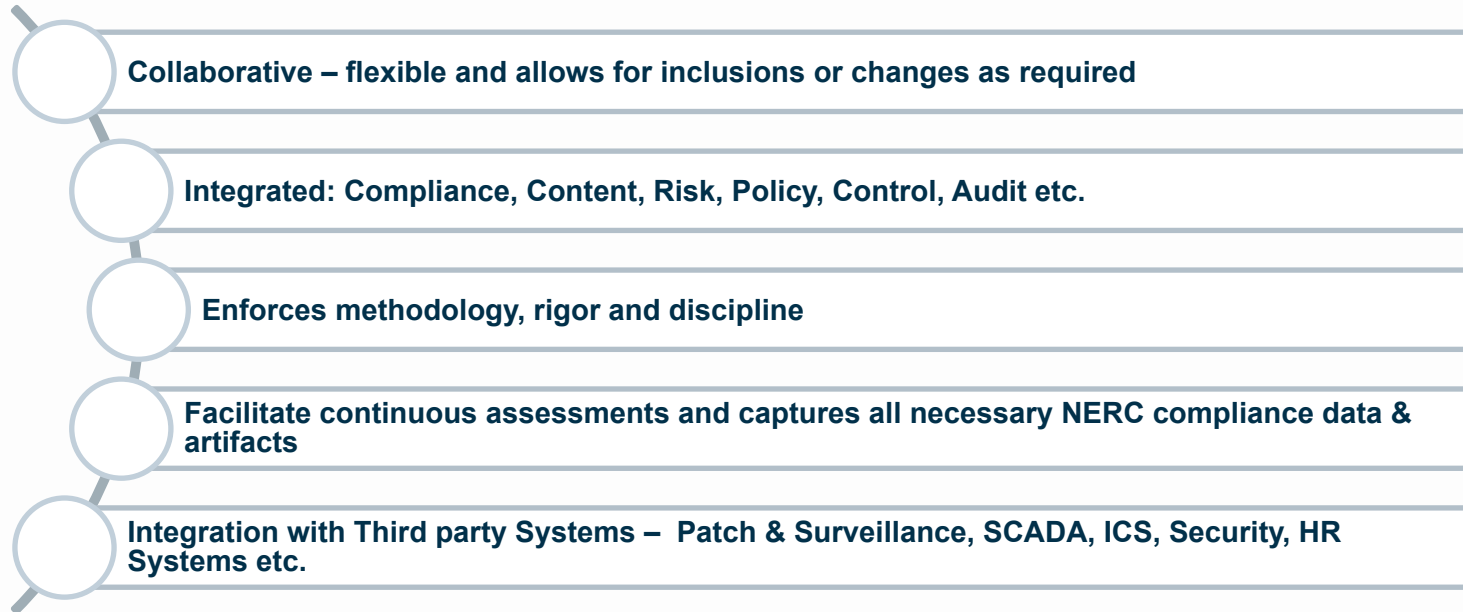


# EUP (Energy and Utility Platform)

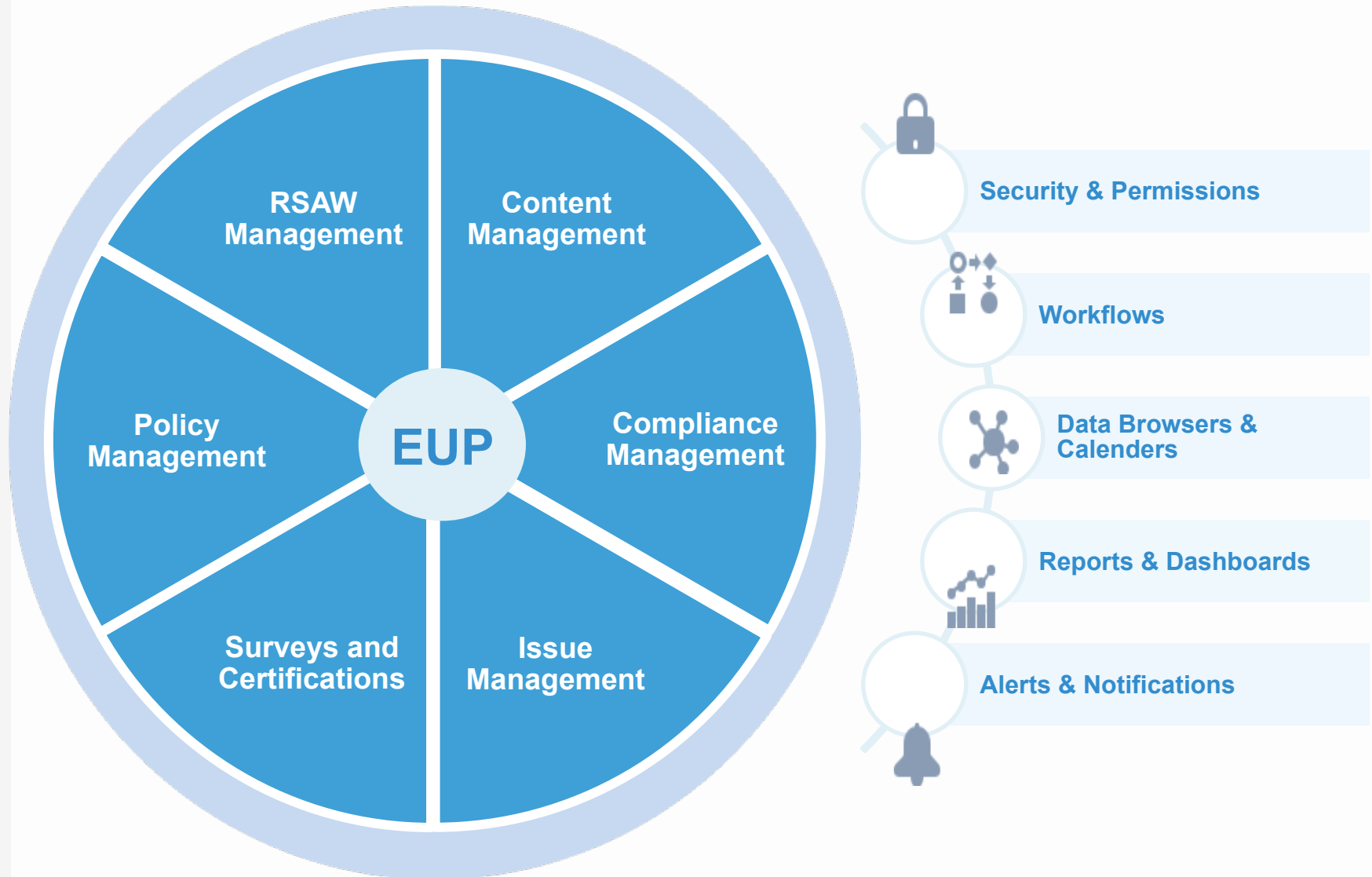


**Shreyank Shrinath  
Kamat**  
Product Manager  
MetricStream

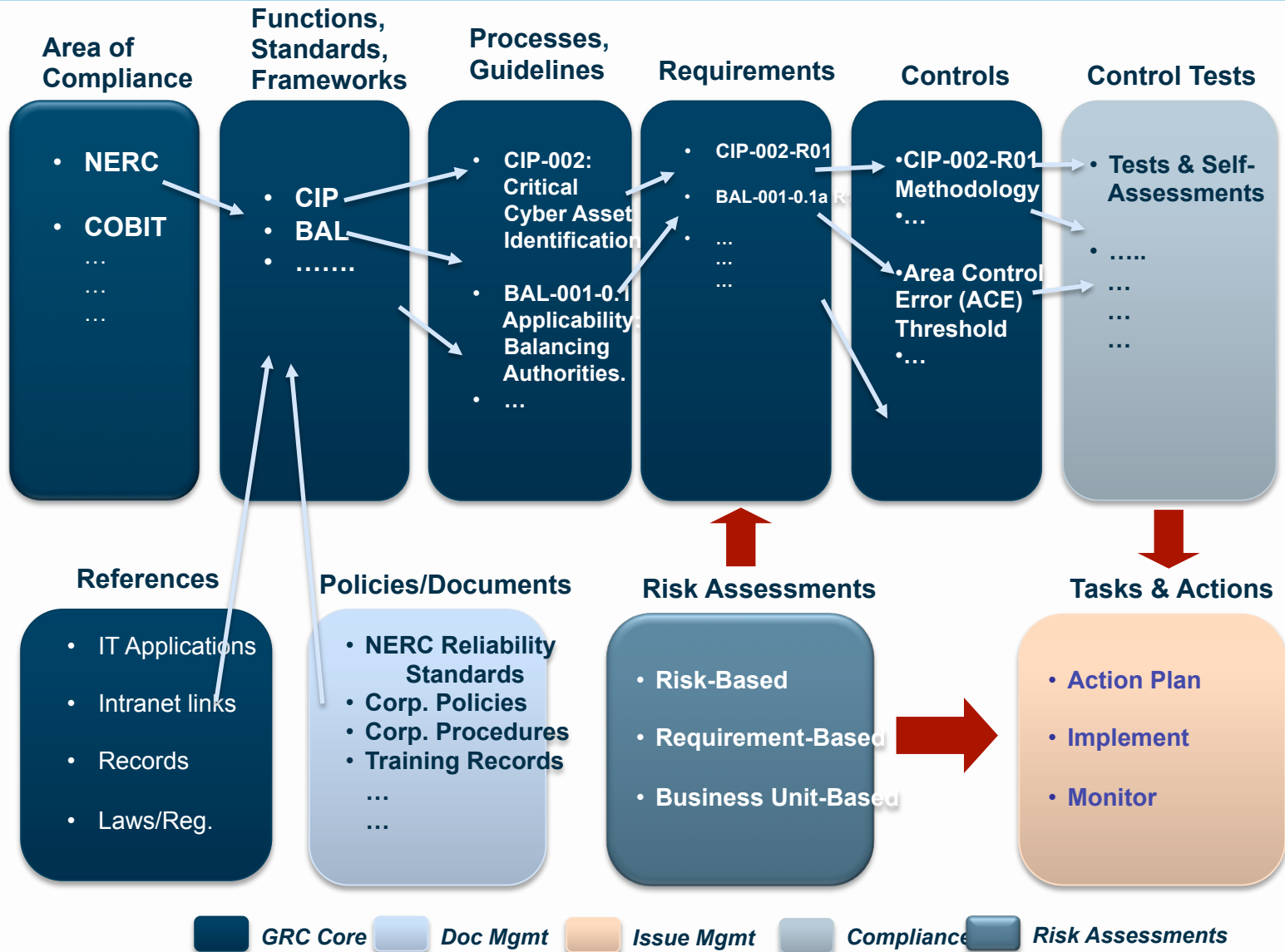
# Effective NERC – CIP Compliance Program



# Key Components: NERC Compliance Management



# A Robust & Flexible Information Model



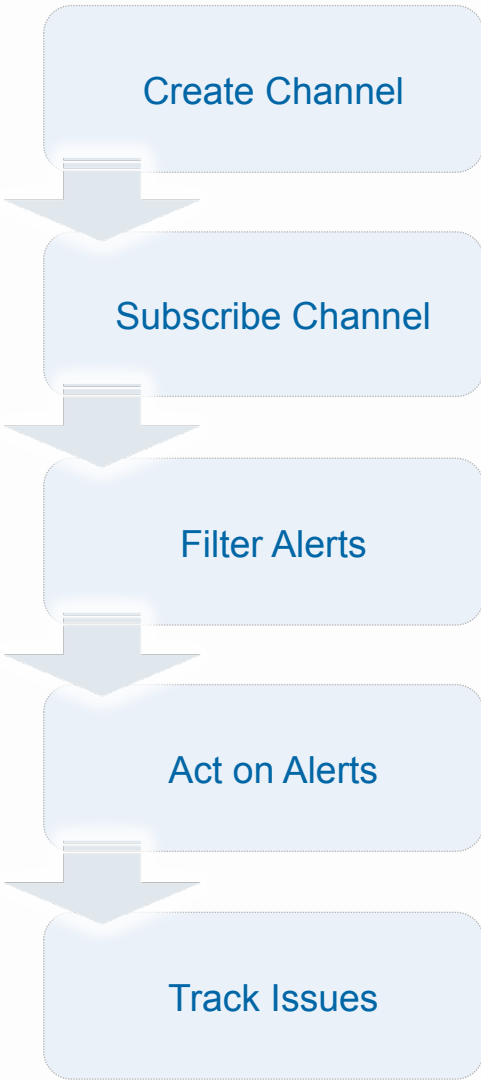
## Setup Content (CIP standards, requirements, controls etc.)



Structure a logical compliance hierarchy, including Areas of Compliance, Standards, Requirements, Controls and Assets.

Configure workflows for managing both internal and external standards, mapping regulations, developing controls, performing compliance audits, preparing and implementing action plans, and identifying and remedying issues.

# Update Content (Regulatory Changes)



**Regulatory Alert Interpretation**

**Interpret Alerts**

**Instructions**  
FERC has identified new rule alerts. Please follow instructions.

1. Click on the title to review alerts.
2. Identify owner who will perform the Risk Assessment.
3. Specify the due by when risk assessment should be completed.
4. Provide your interpretation comments.

Total Rows: 15

Select	Title	Description
<input type="checkbox"/>	<a href="#">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-100-201)</a>	FERC staff has relicensing of the Hydroelectric Project with staff modified adapted to a 2010 the future use of Cooper rivers w protection and environmental impacts must be filed by
<input type="checkbox"/>	<a href="#">Final Rule: FERC issues final rules on NERC's reliability standards</a>	Today's final rule proposed reliability as six of the differences and Terms submitted mandatory reliability to users, owner bulk power system NERC through if procedures. Both

**Electric**

- Annual Charges
- Safety and Inspections
- Environment
- Industry Activities
- General Information
- Hydropower
- Natural Gas
- Oil

**Order No. 1000**

- May 17, 2012 - Item E-1: FERC Denies Rehearing of Transmission Planning and Cost Allocation Rule [News Release](#) | [Commissioners' Statements](#) | [Norris and LaFleur Order No. 1000-A](#) [PDF](#)
- July 21, 2011 - Item E-6: FERC Transmission Planning, Cost Allocation reforms to benefit consumers [News Release](#) | [Fact Sheet](#) [PDF](#) | [Presentation](#) [PDF](#) | [Order No. 1000](#) [PDF](#) (effective)

**Electric Reliability**

- 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](#)
- 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](#) [PDF](#)

**Smart Grid**

- July 19, 2011 - FERC: No sufficient consensus for Smart Grid Interoperability Standards [Decision](#) [PDF](#) | [NIST](#) [PDF](#)
- February 16, 2011 - FERC seeks supplemental comments on Smart Grid Interoperability Standards [Notice](#) [PDF](#) | [Event Details](#)
- December 21, 2010 - FERC staff to hold technical conference on Smart Grid Interoperability Standards on January 31, 2011 [Event](#)

# Test Cyber Security Management Controls

- Define and Manage Controls to protect Cyber Assets
- Manage Password Changes to CCAs
- 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 a web application interface for testing cyber security management controls. The interface is divided into two main sections: "Performed On" and "Performed By".

**Performed On Section:**

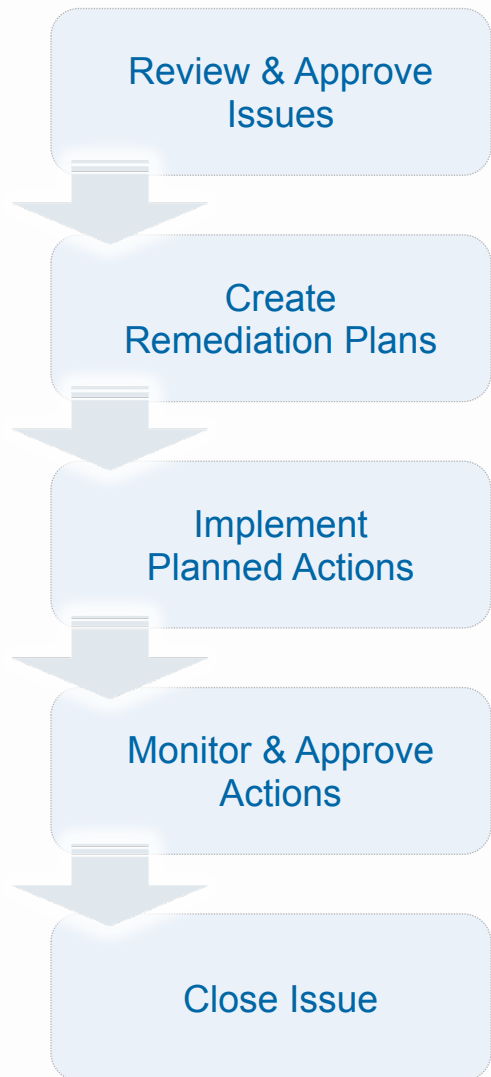
- Navigation tabs: Details, Scheduling, **Performed On**, Performed By, Common Questions/Procedures, Additional Details.
- Section title: **Performed On**
- Form fields: Test/Survey Performed On\*, Control (dropdown), Name\* (Ability to pull back payments), Expected Sample Size.
- Buttons: Delete, Add Item, Delete Last Item, Total Items, Pages: 1 of 1, Total Rows: 1.
- Questions/Procedures (from Library): Vulnerability Scan - Client Laptops.
- Additional Questions/Procedures: (empty field).
- Pre-Test Questions (from Library): Vulnerability Scan - Client Laptops.
- Additional Pre-Test Questions: (empty field).

**Performed By Section:**

- Navigation tabs: Details, Scheduling, Performed On, **Performed By**, Common Questions/Procedures, Additional Details.
- Section title: **Organizations to be Tested/Surveyed/Certified**
- Form fields: Organizations\* (LOB - MidWest Power), Location (New York), To Be Performed On (Ability to pull back payments), Assignment Name (Ability to pull back payments...for LOB - MidWest Power).
- Buttons: Delete, Add Organization, Delete Last Organization, Total Organizations.
- Assign To section: Assign To\* (Tester), Tester (John Jacobs), Test Approver (Karen Kyle), Send Pre-Test Questionnaire To (John Jacobs).
- Scheduling section: Select Based On (Select One dropdown).

## Issue Remediation

---



Review and Approve issues that arise from tests, self-assessments and certifications.

Define one or more Action/Remediation plans to

Document the work done and results and send the implemented Actions for review and approval.

Monitor the status and progress of issues and implementation of remediation plans.

Close issues after all the action plan is implemented and approved.



## Surveys and Certifications

---



Create sections and add questions manually or from the GRC library under every questionnaire.

Initiate a Survey or a Certification by choosing a questionnaire and selecting respondents and approvers.

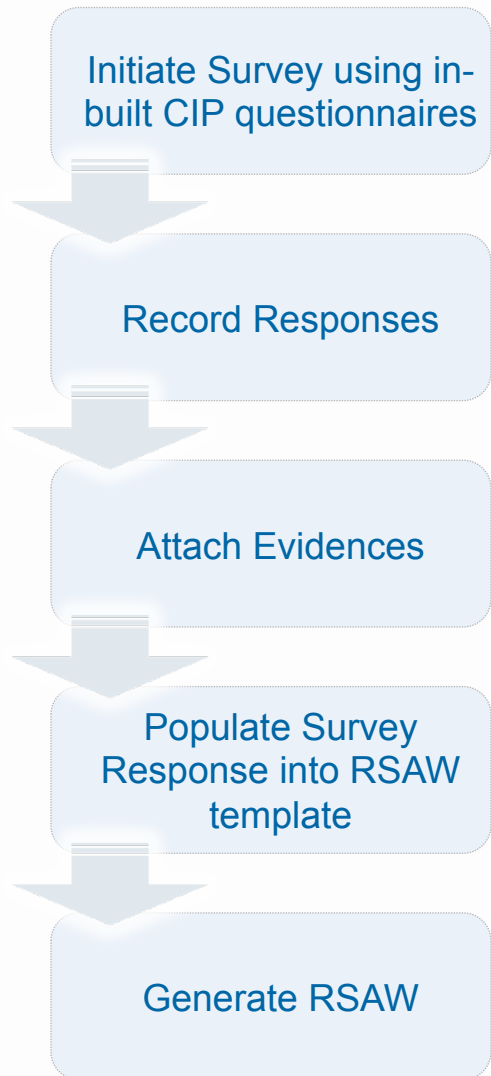
File responses or collaborate with other respondents for responses.

Collate the Survey responses, Approve and sign-off the assessments and key compliance program data.

Add Findings/Issues to capture non-conformance.

## RSAW Management

---



Select a CIP questionnaires and initiate survey to one or more users.

File responses or collaborate with other respondents for responses.

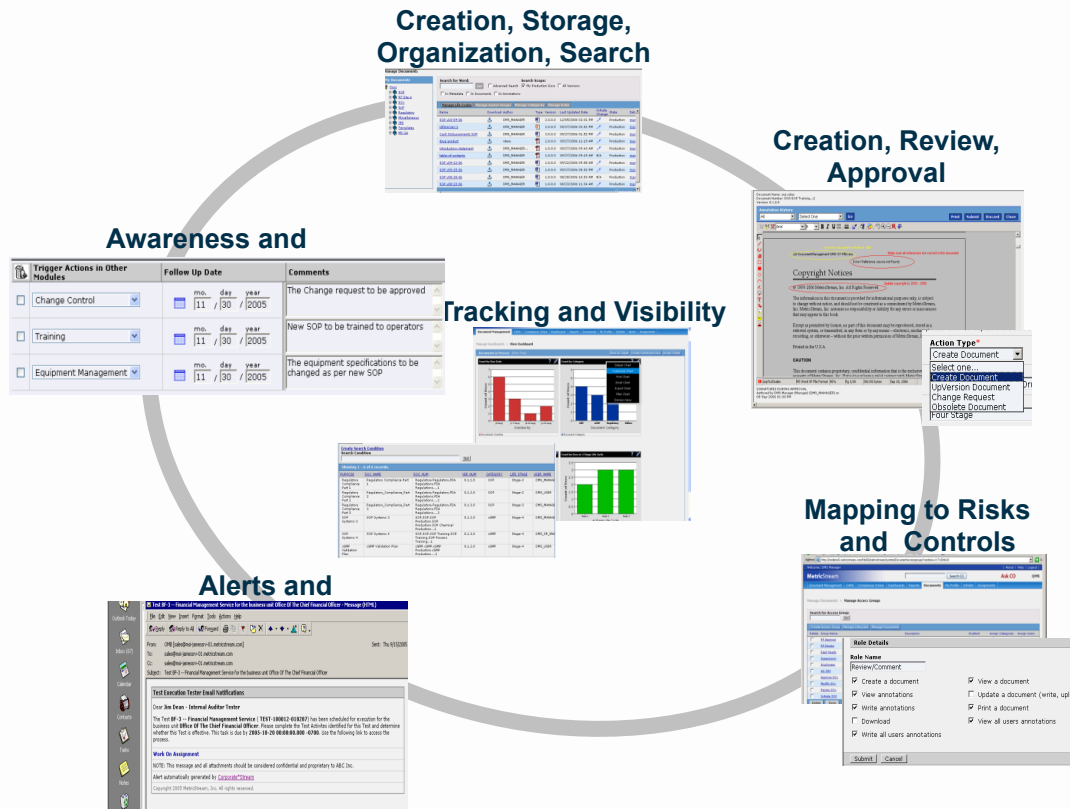
Attach Evidence to the survey from the GRC library or from a previous survey or from the local system.

Select the survey response and populate the same in the in-built RSAW template.

Generate and download the completed RSAW in word format for editing.

# Enforce Policies to Effectively Manage Compliance

- 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 & Critical Assets
- Track NERC version and Migration check
- Monitor NERC Compliance Audit Readiness
- Regulatory Filings, Certifications

The screenshot displays the MetricStream EUP interface, which is used for monitoring and reporting on Energy Utility Programs. The interface is divided into several sections:

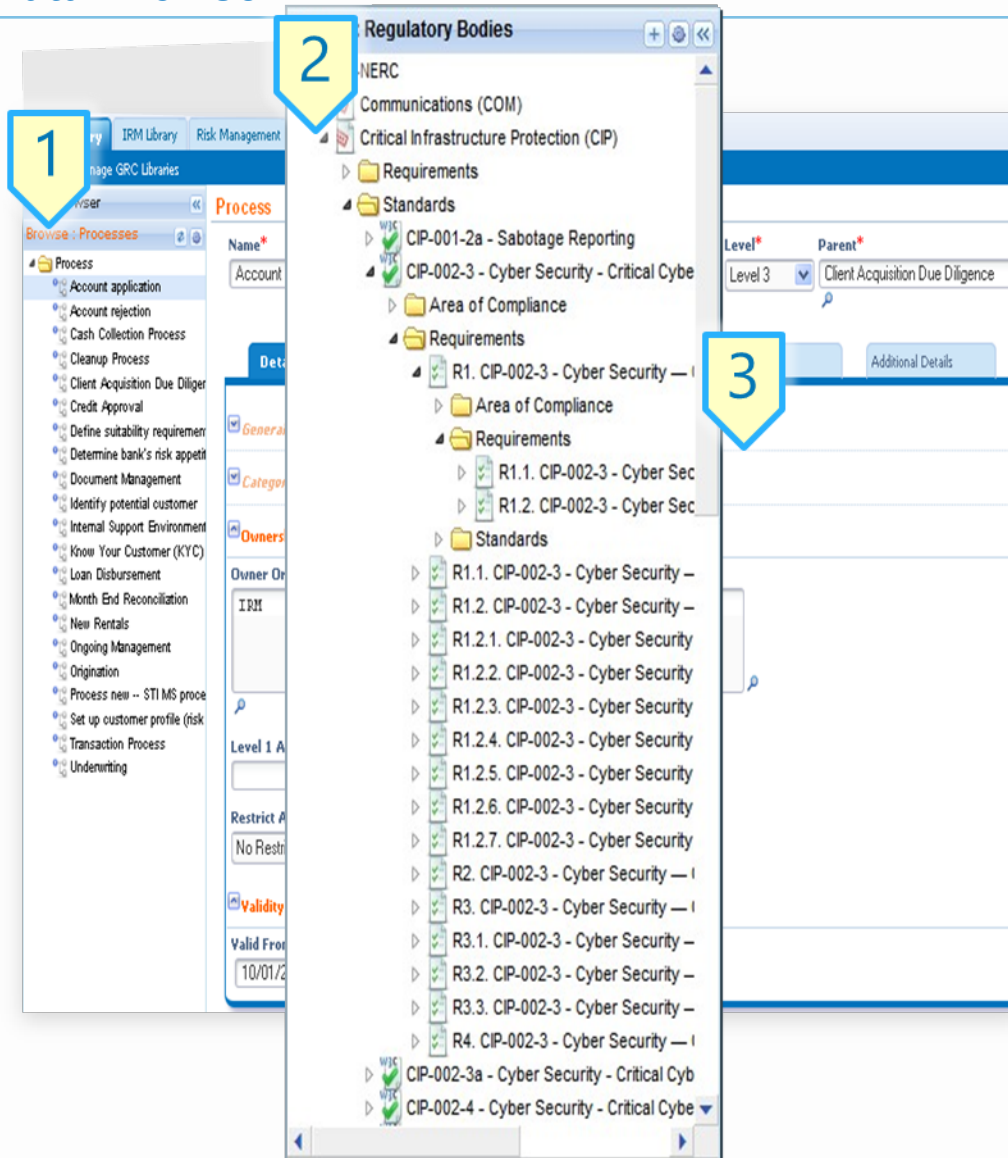
- EUP Overview:** This section provides a high-level summary of the program. It includes two bar charts:
  - Count By Testing Results:** A bar chart showing the distribution of testing results, with 'Pass' being the dominant category.
  - Issue Status:** A bar chart showing the distribution of issue statuses, with 'Open' being the most frequent.
- Requirement Test Details:** A table listing various requirements and their test results. The table includes columns for Requirement, Parent, Test Plan Name, Owner, Frequency, Assessment Name, Status, Completed On, Due Date, Due Days, Assessment, Tested By, and Test Approver.
 

Requirement	Parent	Test Plan Name	Owner	Frequency	Assessment Name	Status	Completed On	Due Date	Due Days	Assessment	Tested By	Test Approver
CIP-010-1-R1.1	CIP-010-1-R01	CIP-010-1-R1 & R1.1		No Scheduling	CIP-010-1-R1.1.1a	Open	23-SEP-14	23-SEP-14	105	Corporate	MetricStream	
CIP-007-5-R2		CIP-007-5-R5 & R5.1		No Scheduling	CIP-007-5-R2.1a	Open	23-SEP-14	24-SEP-14	0	Corporate	MetricStream	
CIP-007-5-R2		CIP-007-5-R5 & R5.1		No Scheduling	CIP-007-5-R2.1a	Open	23-SEP-14	24-SEP-14	0	Compliance M.	MetricStream	
CIP-002-5-R1.1	CIP-002-5-R01	CIP-002-5-R1 & R1.1		No Scheduling	CIP-002-5-R1.1.1a	Open	23-SEP-14	23-SEP-14	104	Compliance M.	MetricStream	
CIP-002-5-R1		CIP-007-R3 & R3.2		No Scheduling								
CIP-003-5-R1.2	CIP-003-5-R01	CIP-003-5-R1 & R1.1		No Scheduling								
CIP-003-5-R1.1	CIP-003-5-R01	CIP-003-5-R1 & R1.1		No Scheduling								
CIP-003-5-R3		CIP-003-R3 & R3.1.1		No Scheduling								
- EUP Overview Report:** A detailed report showing the area of compliance and the performance on various metrics. The report lists several areas of compliance, including Personnel Performance, Training, and Qualifications (PER), Emergency Preparedness and Operations (EOP), Modeling, Data, and Analysis (MOD), Transmission Planning (TPL), Communications (COM), Protection and Control (PRC), Voltage and Reactive (VAR), and Interconnection Reliability Operations and Coordination (R).
- Issues:** This section provides a comprehensive view of the program's issues. It includes:
  - Issue Aging Report:** A table showing the number of issues by source and due date.
 

Issue Source	Overdue			Due			Total
	This Month	Past 3 Months	Beyond 3 Months	This Month	Within 4 Months	Beyond 4 Months	
Ad-Hoc	0	7	0	0	0	0	7
Audit	0	1	0	0	0	0	1
GRC Intelligence	0	1	0	0	0	0	1
Risk Assessment	0	6	0	0	0	0	6
  - Issue Status:** A bar chart showing the distribution of issue statuses, with 'Action Plan Implementation' being the most frequent.
  - Issue Rating:** A bar chart showing the distribution of issue ratings, with 'High' being the most frequent.
- Issues Table:** A table listing individual issues, including columns for Issue Title, Issue Status, Issue Owner, Issue Priority, Issue Due Date, Issue Initiator, First Identified, Progress Status, Exception Type, Source Type, Issue Type, No. of Issues, and Core Object.
 

Issue Title	Issue Status	Issue Owner	Issue Priority	Issue Due	Issue Initiator	First Ident.	Progress S...	Exception Type	Source Type	Issue Type	No. of...	Core Obj...
Customer Records not maintained in first...	Closed	Barry Brown	High	Oct-16-2014	John Jacobs			Operating Exc...	Test Execut...	Data Breach	1	
Financial Records not maintained	Remediated	Stella Stone	High	Oct-21-2014	Troy Tory			Operating Exc...	Risk Asses...	Control Fail...	1	
Finding-4	Action Plan Implem...	Fred Flint	High	Nov-25-2...	Mike Morton				Risk Asses...	Control Fail...	1	
Finding-1	Action Plan Implem...	Quinter Grau	High	Nov-25-2...	Stan Smith				Risk Asses...	Control Fail...	1	

# Data Browser



1 Search and View libraries from a 360° angle.

2 Access library reports

3 Access Dashboards and Charts corresponding to the every library.

## 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 minutes/ hours.
- ⦿ Have real-time visibility into business to avoid compliance concerns

# About MetricStream

## Vision

Integrated Governance, Risk and Compliance for Better Business Performance

## Solutions

- NERC CIP Compliance
- Risk Management
- Business Continuity Management
- IT GRC
- Audit Management
- Supplier Governance
- Quality Management
- EHS & Sustainability
- Governance & Ethics
- Content and Training

## Partners



## Organization

- Over 1,800+ employees
- Headquarters in Palo Alto, California with offices worldwide
- Over 350 enterprise customers
- Privately held – Backed by global leading VCs, Sage View Capital, Goldman Sachs

## 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 GRC SUMMIT 2015 – November 10-11, London, UK

MetricStream  
**GRC**  
SUMMIT **2015**  
November 10 - 11, 2015  
E U R O P E

## Maximize Business Performance

KNOW MORE ↻

 Royal Lancaster Hotel,  
London, UK

 November 10 - 11, 2015

200+  
Attendees

30+  
Sessions

35+  
Speakers

2  
Days

For more information, please visit <http://www.grc-summit.com/europe/>



## Q&A



**Karl Perman**  
VP Member Services  
EnergySec  
Email: [karl@energysec.org](mailto:karl@energysec.org)



**Shreyank S. Kamat**  
Product Manager  
MetricStream  
Email: [shreyank.kamat@metricstream.com](mailto:shreyank.kamat@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/events/webinars>**

# 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