

2017 Approved Audit Plan

Internal Audit and Corporate Risk Management Department

Approved: February 7, 2017

Approved Two Year Internal Audit Engagement Plan

2017 Approved Internal Audit Engagement Plan	
Operational Areas	Corporate Areas
NERC Standards Independent Audit*	NERC Payroll Audit
Regional Entity Event Analysis Process Audit	NERC Confidential Information Audit
Regional Entity Business Continuity Audit	
NERC Compliance Assurance Inherent Risk Assessment Oversight Audit	
Statistical Analysis Supporting the State of the Reliability Report Audit	
CRISP Audit*	

2018 Approved Internal Audit Engagement Plan	
Operational Areas	Corporate Areas
RE Technical Feasibility Exception Audit	NERC IT Access Review Process Audit
NERC RE Registration Oversight Audit	NERC Budget Planning Process (ROP Section 1100) Audit
NERC Handling and Processing Directives Audit	RE Budget Planning Process (ROP Section 1100) Audit
RE Data Request (ROP Section 1600) Audit	
CRISP Audit*	
NERC RE CIP Oversight Audit	
NERC Business Continuity Audit	

Note: The audit descriptions are provided in Appendix A.

**Required by the Rules of Procedures, contractual agreement or other mandate.*

Risk Management Activities Detail

2017 Risk Management Activities	
NERC Enterprise Risk Management	ERO Enterprise Risk Management
Quarter 1	
<ul style="list-style-type: none"> • Conduct 2017 NERC enterprise risk assessment. 	<ul style="list-style-type: none"> • ERO Enterprise risk management working group identification and consolidation of Enterprise-wide controls.
Quarter 2	
<ul style="list-style-type: none"> • Report NERC enterprise risk assessment results to EWRC (per EWRC mandate). 	<ul style="list-style-type: none"> • Review ERO Enterprise risk assessment results with ERO Enterprise Executives.
Quarter 3	
	<ul style="list-style-type: none"> • Review ERO Enterprise risk assessment results with EWRC, NERC and Regional Boards of Directors/Trustees.
Quarter 4	
<ul style="list-style-type: none"> • Perform re-evaluation of NERC risk assessment results. • Propose 2018 audit plan to the EWRC based on risk assessment results. 	<ul style="list-style-type: none"> • Perform re-evaluation of ERO Enterprise risk assessment results. • Propose 2018 audit plan to the EWRC based on risk assessment results.

Appendix A – Audit Description

Preliminary Audit Name	Preliminary Audit Description	Resources
2017 Approved Operational Audits		
NERC Standards Independent Audit	Per requirements set forth in ROP Section 405, conduct an independent audit to determine whether the Standards development process adheres to the Rules of Procedures, Standards Process Manual and other governing documents.	Internal / Contractor
Regional Entity Event Analysis Process Audit	Assure that the RE Event Analysis programs adhere to the delegation agreements, Rules of Procedures and other guiding documents.	Internal
Regional Entity Business Continuity Review	Determine the nature and extent of RE business continuity processes, in relations to delegated functions.	Internal
NERC Inherent Risk Assessment (IRA) Oversight Audit	Assess whether NERC is adequately performing oversight activities to ensure that the IRA's developed by the Regional Entities are conducted in accordance with established criteria, procedures, training and guidance to effectively identify areas of focus and the level of effort needed to monitor compliance with enforceable Reliability Standards.	Internal
Statistical Analysis Supporting the State of Reliability Report	Evaluate whether the processes and internal controls exist for statistical inferences made in the State of Reliability Report. The audit will include a review of the statistical assumptions utilized.	Contractor
ES-ISAC CRISP Independent Audit	In accordance with the CRISP contract, an annual independent inspection of CRISP data handling.	Contractor
2017 Approved Corporate Audits		
NERC Payroll Audit	Evaluate whether the NERC payroll process is effective and operating as intended. This audit will include (but not limited to) system user access, maintaining confidential information and reviews and approvals.	Internal
NERC Confidential Information Audit	Follow-up audit NERC's process and internal controls to ensure confidential information is maintained in accordance with the ROP and company policies and procedures. The audit will also include an evaluation of the document management initiative in enabling an effective control environment in this area.	Internal

2018 Approved Operational Engagements		
RE Technical Feasibility Exception (TFE) Audit	Evaluate whether the RE audit team are adhering to the ROP and revised NERC guidance associated with the TFE process.	Internal
NERC RE Registration Oversight Audit	Assess whether NERC is adequately performing oversight activities to ensure that RE Registration processes adhere to the ROP and established criteria, procedures, training and guidance.	Internal
NERC Handling and Processing Directives Audit	Assess whether NERC maintains processes and internal controls for compiling, disposing and reporting FERC directives.	Internal
RE Data Request (Section 1600 ROP) Audit	Ensure that the REs adhere to ROP Section 1600 and established policies, procedures and guidelines.	Internal
NERC RE CIP Oversight Audit	Assess whether NERC is adequately performing oversight activities to ensure that RE CIP auditor adhere to the ROP and established criteria, procedures, training and guidance.	Internal
ES-ISAC CRISP Independent Audit	In accordance with the CRISP contract, an annual independent inspection of CRISP data handling.	Contractor
2018 Approved Corporate Audits		
NERC IT Access Review Process Audit	Evaluate NERC's process to ensure that the appropriate employee and vendors have access to applications, networks and tools. Determine whether NERC's access review ensures unique and special access is appropriately evaluated and approved.	Internal
NERC Budget Planning Process Audit	Ensure that the REs adhere to ROP Section 1100 and established policies, procedures and guidelines.	Internal
RE Budget Planning Process Audit	Ensure that the NERC adheres to ROP Section 1100 and established policies, procedures and guidelines.	Internal
NERC Business Continuity Audit	Assess NERC's newly implemented business continuity process, including, but not limited to, the confidentiality, security and availability of IT capabilities, actual or planned employee training on the business continuity plan, incorporation of procedures to address mitigation of reputational risk (e.g., media relations as required) and coordination with third parties (as required).	Internal