

New York Power Authority *Internal Audit (IA) Update*

December 11, 2014

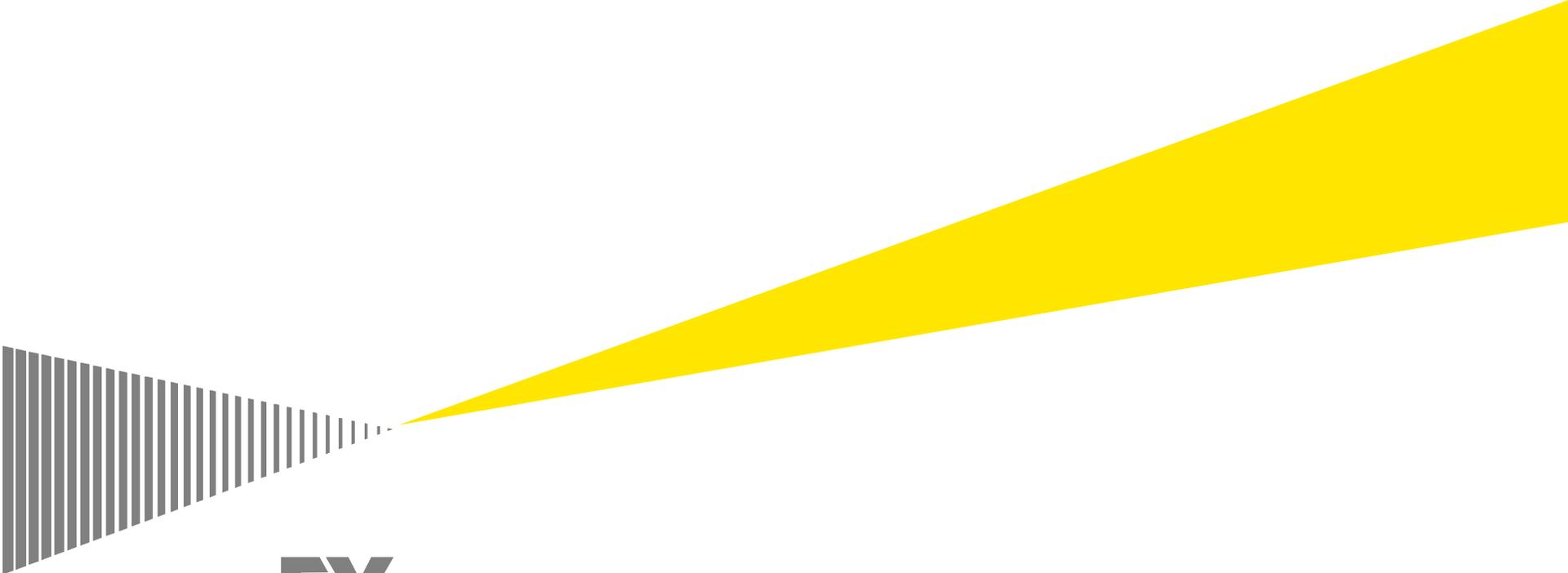


Table of Contents

- ▶ Executive Summary
- ▶ Status of 2014 IA Plan Execution
- ▶ 2015 Report Rating Process
- ▶ 2015 Risk Assessment and Proposed IA Plan
- ▶ Appendix A – Proposed 2015 IA Plan
- ▶ Appendix B – 2014 IA Plan

Executive Summary

- ▶ Receiving continued cooperation from NYPA Senior Staff and Department Managers with regard to the IA Teaming arrangement with EY
- ▶ Search is ongoing for CAE, Audit Manager (1), Supervisory Senior IT Auditor (1), and Senior Auditors (2) vacancies;
 - An offer has been extended for one of the Senior Auditor positions
- ▶ IA department improvements are in progress, including:
 - Report and observation rating categories and criteria were presented and agreed with the Executive Management Committee (EMC) members and will be instituted for the 2015 IA plan
 - Feedback has been developed on enhancements to the internal audit charter and suggested amendments pending review by the CAE/management and the Audit Committee prior to implementation
- ▶ The proposed 2015 IA plan has been developed and is pending discussion/approval

Status of 2014 IA Plan

- ▶ The following reflects the status of audits in the 2014 IA Plan:

Status	As of September 8 th	As of October 15 th	As of November 17 th	As of December 31 st (projected)
Report Issued	7	7	12	22
Report Pending Issuance	4	10	10	9
Fieldwork In Progress	13	9	8	5
Audit Planning	9	10	6	-
Not Started	6	2	-	-
Moved to 2015 IA Plan *	-	1	3	3
Total	39	39	39	39

Note*: NYISO Energy Settlements – Generation, Network ITGC and Load Forecasting have been postponed to 2015 due to system / process changes.

- ▶ Since the last Audit Committee Meeting on October 15, 2014, the IA Department has completed the following audits:
 - Operational Planning – Asset Investment Planning (OPR14070) - 2014
 - Purchasing/Warehousing – Niagara (FIN14950) - 2014
 - Purchasing/Warehousing – St. Lawrence (FIN14600) - 2014
 - Cash Management & Treasury Operations (FIN14120) – 2014
 - Social Media Governance (OPR14090) - 2014
- ▶ Fieldwork wrap-up and reporting for remaining 2014 audits will not impact the focus and timing of the 2015 IA Plan through adjustments to resource planning and coordination.

2015 Report Rating Process

- ▶ The report rating process was presented to the EMC and agreed upon in October 2014
- ▶ Report ratings and observation ratings will be utilized beginning with audits on the 2015 IA Plan
- ▶ Management action plans will be monitored based on ratings

Overall Report Rating	Description	Aggregation
Good 	Our procedures resulted in no significant findings related to the design of internal controls or to the proper functioning of controls as designed.	There are minimal observations which are all rated low.
Satisfactory 	Our procedures resulted in no significant findings related to the design of internal controls or to the proper functioning of controls as designed. Controls are generally functioning as intended, but some changes are necessary to make the control environment more efficient and effective.	Observations are predominantly rated low.
Improvement Needed 	Our procedures resulted in findings, some of which are significant, related to the design of internal controls and/or to the proper functioning of controls as designed. These control deficiencies should be addressed by management to further strengthen the system of internal control.	Observations are predominantly rated moderate and/or may have high-rated observations.
Unsatisfactory 	Based on our procedures performed, either the design of internal controls does not appropriately mitigate specific identified risks or numerous exceptions were noted in our testing indicating that controls were not functioning as designed. Management should take immediate action to address these findings by instituting new control procedures or modifying existing procedures.	Observations are predominantly rated moderate and/or high.

Individualized Observation Ratings	
Low	A minor weakness that when addressed will strengthen the control process and/or is of lower importance to business success/achievement of goals.
Moderate	Moderate risk of an error or incident occurring that may contribute to the non-achievement of a control objective and/or is important for business achievement of goals. Management action is required to address the identified deficiencies.
High	High risk of an error or incident occurring that may contribute to the non-achievement of a control objective and/or is a key focus for business success/achievement of goals. Immediate management action needs to be taken to address the identified deficiencies.

2015 Risk Assessment and Proposed IA Plan

Risk Assessment & IA Planning Overview

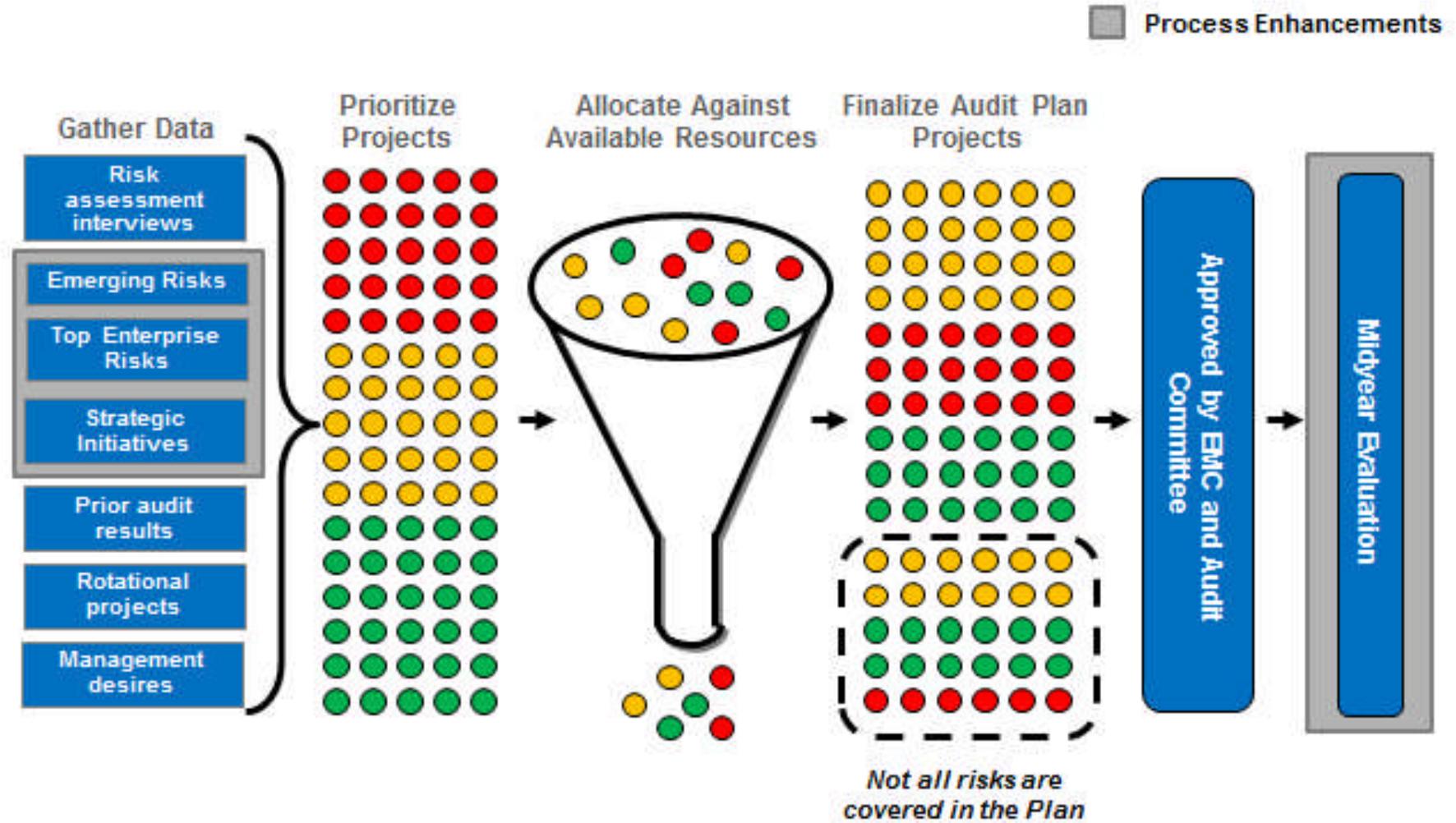
- ▶ Risk Assessment Process:
 - Interviewed 56 individuals across management and the Audit Committee
 - Obtained feedback on strategic and critical business objectives and the risks to achieving those objectives
 - Reviewed the strategic plan, emerging risks and industry trends
 - Identified and prioritized risk areas based on risk assessment criteria to develop the proposed internal audit plan

- ▶ Types of Internal Audit Projects Proposed:
 - **Audit:** Projects designed to evaluate the design and effectiveness of current processes and related control activities; generally considered a “look-back” review. Consideration will also be given to leading practices within the current processes.
 - **Consultative:** Projects designed to evaluate the design of new processes and related control activities; generally considered an assessment of future state operations. Consideration will also be given to leading practices within the new processes or initiatives.

- ▶ Risk Area Coverage:
 - **Financial Risk:** May result in a financial impact
 - **Operational Risk:** May result in an interruption to business operations
 - **Compliance Risk:** May result in compliance and/or legal issues
 - **Strategic Risk:** May impact corporate initiatives and/or reputation

2015 Risk Assessment and Proposed IA Plan

Risk Assessment & IA Planning Overview



2015 Risk Assessment and Proposed IA Plan

Key Themes for Discussion

► Summary of the proposed 2015 IA Plan (Appendix A) :

Lead Business Unit	Q1	Q2	Q3	Q4	Total
Business Services	3	4	3		10
Enterprise Shared Services	6	6		3	15
Law Department		1			1
Public & Regulatory Affairs				1	1
Operations		2		3	5
Economic Development & Efficiency		1	1		2
Total	9	14	4	7	34

Audit Type	FY15	FY14
Non-IT *	19	22
Integrated	6	5
IT	9	9
Total	34	36

Subject-Matter ("SM") Involvement	FY15	FY14
SM Led	9	9
SM Support	12	6
IA Led	13	21
Total	34	36

*Note that several of the non-IT audits will include a limited review of IT general controls, segregation of duties and access rights.

Appendix A – Proposed 2015 IA Plan

Internal Audit Plan

#	Proposed Audit Area	Project Type	Business Unit	Audit Type	Audit Description / Preliminary Audit Scope Target	Target Timing	Planned Resource Involvement
1	Cyber Security - Maturity Assessment	Audit	Enterprise Shared Services	IT	Perform a cyber-security maturity assessment based on ES-C2M2	Q2	Subject Matter Led
2	Cyber Security - Network Discovery	Audit	Enterprise Shared Services	IT	Perform a network discovery assessment which will include but not be limited to, a logical configuration review of touch points between IT and OT and firewall rule-set review.	Q1	Subject Matter Led
3	Pre Implementation review: CIMS to Maximo Migration	Audit	Enterprise Shared Services	IT	Perform a pre implementation review of the data conversion from CIMS to Maximo and appropriateness of technical security role set up.	Q1	Internal Audit Led
4	Incident Response Plan Phase 2	Audit	Enterprise Shared Services	IT	Based on the results of the 2014 incident response internal audit report, perform a simulated attack and assess how the incident response plan is executed in practice.	Q4	Internal Audit Led
5	Access Control Repository	Audit	Enterprise Shared Services	IT	Perform a pre-implementation review of the access control repository and perform a walkthrough and testing of the new process post implementation to assess design and effectiveness of the new controls related to the new access management process	Q1	Internal Audit Led

Appendix A – Proposed 2015 IA Plan

Internal Audit Plan

#	Proposed Audit Area	Project Type	Business Unit	Audit Type	Audit Description / Preliminary Audit Scope Target	Target Timing	Planned Resource Involvement
6	Network ITGC	Audit	Enterprise Shared Services	IT	Test and evaluate the NYPA Network to determine if it is adequately protected from unauthorized access, use, disclosure or modifications, damage or loss using best security practices. Review, test and evaluate the controls and control procedures over the changes to network software and their testing and approval by users prior to their placement in production.	Q1	Internal Audit Led
7	Data Loss Prevention	Audit	Enterprise Shared Services	IT	Evaluate data loss prevention practices to determine whether a data classification process is in place and evaluate management's data classification scheme and capabilities to protect data across the full data lifecycle, including sharing of data with third parties.	Q2	Subject Matter Led
8	Ariba Procurement Solution	Consultative	Business Services	IT	Perform a pre-implementation review of the SAP cloud based solution for Sourcing, Contracts and Suppliers to facilitate NYPA Procurement activities.	Q3	Subject Matter Support
9	NYPA Customer Portal	Audit	Enterprise Shared Services	IT	Perform pre implementation review of the web-based NYPA customer portal to assess and evaluate the effectiveness of the controls around complete and accurate interface of the customer data including demographic, billing, payment data, and the usage data.	Q4	Subject Matter Support

Appendix A – Proposed 2015 IA Plan

Internal Audit Plan

#	Proposed Audit Area	Project Type	Business Unit	Audit Type	Audit Description / Preliminary Audit Scope Target	Target Timing	Planned Resource Involvement
10	NERC CIP 5 Collaboration	Audit	Operations	Integrated	Assist in performing a readiness assessment for NERC CIP 5 Compliance, including but not limited to, governance over asset maintenance, procedures for new asset additions and completeness and accuracy of asset classifications utilized. Assist the technical compliance group in performing Reliability Standards Compliance (RSC) Assessments internally.	Q2	Subject Matter Led
11	Asset Accounting / Maximo Post Implementation	Audit	Enterprise Shared Services	Integrated	Utilizing analytics perform an assessment of the asset management lifecycle to determine processes, procedures and controls in place from the point at which an asset is entered into Maximo, and configured for depreciation. Assess whether process and controls are operating as designed, and perform post implementation procedures of the Maximo application.	Q2	Internal Audit Led

Appendix A – Proposed 2015 IA Plan

Internal Audit Plan

#	Proposed Audit Area	Project Type	Business Unit	Audit Type	Audit Description / Preliminary Audit Scope Target	Target Timing	Planned Resource Involvement
12	IT Project Management Office ('PMO')	Audit	Enterprise Shared Services	Integrated	Evaluate the adequacy and effectiveness of project management governance controls within IT. This should include the setting and monitoring of projects against milestones throughout the project lifecycle, processes and procedures followed by IT to accept or reject capital project requests (i.e., business requirements), new system governance (i.e., who can procure a system, who must approve the procurement, when IT gets involved), communication with the business, timelines, prioritization, etc.	Q1	Subject Matter Support
13	Energy Settlements, Scheduling and Load Forecasting	Audit	Economic Developm't & Efficiency	Integrated	Assess the processes and controls related to Market Analysis & Administration groups' NYISO scheduling processes. Specifically, assess the current state processes and controls, post-implementation of the automated Scheduling Automation project. Additionally, assess the processes and controls related to the cross-functional area ISO generation, physical transaction, and financial transaction settlements processes, including but not limited to governance of the functions, organizational alignment of the functions, and the processes and controls of the respective settlements functions. In addition, assess the processes and controls related to the Market Analysis & Administration group's development of customer load forecasts. Specifically, model/tool governance, data input controls, data output controls, general IT controls.	Q2	Subject Matter Led

Appendix A – Proposed 2015 IA Plan

Internal Audit Plan

#	Proposed Audit Area	Project Type	Business Unit	Audit Type	Audit Description / Preliminary Audit Scope Target	Target Timing	Planned Resource Involvement
14	Meter to Cash	Audit	Business Services	Non-IT	Perform an end to end assessment of the meter to cash process and evaluate the design and operating effectiveness of controls as identified. This assessment will include but not be limited to the systems used throughout the billing process, data interfaces between those systems and controls in place to secure accurate billing to customers.	Q1	Subject Matter Support
15	Y49 Cables	Audit	Operations	Non-IT	Perform a review of monitoring actions in place to prevent a failure in the Y49 cables and verify the risk is adequately mitigated.	Q2	Subject Matter Support

Appendix A – Proposed 2015 IA Plan

Internal Audit Plan

#	Proposed Audit Area	Project Type	Business Unit	Audit Type	Audit Description / Preliminary Audit Scope Target	Target Timing	Planned Resource Involvement
16	Fleet Operations	Audit	Enterprise Shared Services	Non-IT	Perform an end to end assessment of fleet operations including governance over the fleet operation, usage of each type of fleet vehicle, fleet maintenance, inventory management and roles and responsibilities of fleet personnel. Verify compliance with policies and procedures and measure preparedness against the asset management system (e.g., Maximo).	Q2	Internal Audit Led
17	Contractor Tenure	Audit	Business Services	Non-IT	Assess the current process, policies and procedures in place for utilizing contractors, including but not limited to an analysis of the volume of contractors used vs. full-time employees (FTE's), the decision making process for using contractors vs. hiring FTE's, and compliance with Department of Labor requirements.	Q2	Subject Matter Support
18	Budgeting and Forecasting	Audit	Business Services	Non-IT	Review the adequacy and effectiveness of the current budgeting process for both the operating and capital budget such as who is responsible for making budgeting decisions, how departments monitor budgets throughout the year (i.e., KPI's), how items within the budgets are prioritized and approval layers in place. In addition, review the adequacy and effectiveness of operating controls associated with the long range financial plan and ongoing operating forecasts including quality control procedures and disclosure of assumptions used.	Q2	Subject Matter Support

Appendix A – Proposed 2015 IA Plan

Internal Audit Plan

#	Proposed Audit Area	Project Type	Business Unit	Audit Type	Audit Description / Preliminary Audit Scope Target	Target Timing	Planned Resource Involvement
19	Energy Efficiency Controls	Consultative	Economic Developm't & Efficiency	Non-IT	Perform a pre-implementation assessment of the new energy efficiency program initiatives to identify whether adequate business controls are in place, or control gaps are identified which need to be addressed.	Q3	Subject Matter Led
20	Construction Projects	Audit	Business Services	Non-IT	Perform a governance and controls assessment and evaluation of controls in place throughout the duration of a construction project (i.e., from initiation of the project through project completion), including project management activities.	Q2	Subject Matter Led
21	Vendor Contracts Audit	Audit	Business Services	Non-IT	For selected procurement contracts, determine that services provided by the vendor are in agreement with contract terms and conditions.	Q2	Internal Audit Led

Appendix A – Proposed 2015 IA Plan

Internal Audit Plan

#	Proposed Audit Area	Project Type	Business Unit	Audit Type	Audit Description / Preliminary Audit Scope Target	Target Timing	Planned Resource Involvement
22	Compensation & Benefits	Audit	Enterprise Shared Services	Non-IT	Evaluate the adequacy and effectiveness of internal controls throughout the benefits program and newly developed Merit program and verify compliance with policies and procedures. Perform a benchmarking assessment of benefit options offered to NYPA employees against leading practice.	Q1	Internal Audit Led
23	O&M Cross Functionality	Consultative	Operations	Non-IT	Based on the results of prior year O&M internal audit reports, perform a comparative assessment of the operations across each of the site locations. Identify potential opportunities to enhance operations at the sites and leverage cross functional functionalities.	Q4	Internal Audit Led
24	Information Management	Audit	Enterprise Shared Services	Integrated	Verify that NYPA-wide policies and procedures exist to govern the classification and storage of internal documentation (e.g., usage of LiveLink, classification of confidential, private and public data), and these policies and procedures are adhered to. Verify the legal hold process is being implemented in accordance with Law Department written directives and prior audit recommendations have been implemented.	Q2	Internal Audit Led

Appendix A – Proposed 2015 IA Plan

Internal Audit Plan

#	Proposed Audit Area	Project Type	Business Unit	Audit Type	Audit Description / Preliminary Audit Scope Target	Target Timing	Planned Resource Involvement
25	Physical Security	Audit	Operations	Non-IT	Based on prior year physical security audit results, review the current state of physical security programs including inspections/ monitoring activities, guard services, capital improvement program, etc. impacting all NYPA locations (generation, transmission including substations, headquarters, etc.). Verify compliance with established NYPA policies and procedures and NERC, and remediation of prior year observations.	Q4	Internal Audit Led
26	IT/OT Integration at Sites	Consultative	Enterprise Shared Services	Integrated	Perform an assessment to understand how the IT/OT integration efforts have affected site operations. Understand how roles and responsibilities should be operating at the sites under the new model, verify they are operating as intended, and verify controls that have shifted ownership due to the change, are operating as intended.	Q2	Subject Matter Support
27	Strategic Plan Governance and Execution	Consultative	Business Services	Non-IT	Evaluate the adequacy and effectiveness of project management governance controls as it relates to the strategic initiatives, including the corporate communication strategy for the strategic initiatives (i.e., has communication has been effectively received by management), setting and monitoring of projects against milestones throughout the project lifecycle and appropriateness of metrics established at the enterprise, corporate and strategic levels.	Q1	Subject Matter Support

Appendix A – Proposed 2015 IA Plan

Internal Audit Plan

#	Proposed Audit Area	Project Type	Business Unit	Audit Type	Audit Description / Preliminary Audit Scope Target	Target Timing	Planned Resource Involvement
28	Licensing Operations	Audit	Public & Regulatory Affairs	Non-IT	Evaluate processes and controls associated with ensuring compliance with existing licenses (tracking, monitoring and performance), review licensing expenditures and related controls, and verify compliance with established NYPA policies and procedures.	Q4	Subject Matter Led
29	Finance & Accounting Niagara	Audit	Business Services	Non-IT	Review procedures, processes and controls over budget monitoring, accounts payable, payroll, travel and living expenses, and Human Resources, verify compliance with established NYPA policies and procedures and alignment to expectations at Corporate.	Q3	Internal Audit Led
30	Purchasing/Warehousing - BG	Audit	Business Services	Non-IT	Review processes and controls associated with purchasing and warehousing activities and verify compliance with established NYPA policies and procedures.	Q3	Internal Audit Led
31	Travel & Entertainment	Audit	Enterprise Shared Services	Non-IT	Perform a targeted assessment of travel and entertainment expenses on a rotational basis, such as: Procedures, processes and controls over Headquarters Business Expenses; Compliance with established NYPA policies, procedures and guidelines; Processes and controls over contractor expenditures submitted to and paid by NYPA.	Q4	Subject Matter support

Appendix A – Proposed 2015 IA Plan

Internal Audit Plan

#	Proposed Audit Area	Project Type	Business Unit	Audit Type	Audit Description / Preliminary Audit Scope Target	Target Timing	Planned Resource Involvement
32	FERC Dam Safety	Audit	Operations	Non-IT	Perform a detailed review of policies, procedures and controls within the FERC Dam Safety program and verify accuracy and completeness of compliance reports.	Q4	Internal Audit Led
33	Fraud Awareness Risk Assessment	Consultative	Law Dep't	Non-IT	Perform a fraud risk assessment with select levels of management to understand the potential areas of fraud management believes are plausible based on a scale of impact and likelihood, and thus areas that need to be monitored more carefully.	Q2	Subject Matter Support
34	Cost Accounting Study	Consultative	Business Services	Non-IT	Evaluate current processes in place to determine the cost structure of products and how NYPA is recovering their costs. Assess whether current operations have the capacity to adapt to new programs and products, such as those proposed by the customer solutions initiative.	Q1	Subject Matter Led

Appendix B – 2014 IA Plan

Ref.	Audit #	Audit	Business Unit	Audit Type	Issuance Date
Report Issued: 12					
1	OPR14016	Physical Security – St. Lawrence	Operations	Operational/Financial	03/14/14
2	OPR14110	Environmental, Health & Safety Audit Programs	Operations	Operational/Financial	03/11/14
3	IS014730	Patch Management	Enterprise Shared Services	Information Technology	06/19/14
4	OPR14007	Revenue Requirements – Hydro Customers	Business Services	Operational/Financial	07/08/14
5	FIN14100	Headquarters Accounts Payable	Business Services	Operational/Financial	08/20/14
6	OPR14017	Central Region O&M	Operations	Operational/Financial	09/02/14
7	FIN14113	Headquarters ProCard Expenses	Various	Operational/Financial	09/03/14
8	FIN14120	Cash Management & Treasury Operations	Business Services	Operational/Financial	10/23/14
9	OPR14070	Operational Planning - Asset Investment Planning	Operations	Operational/Financial	10/28/14
10	FIN14950	Purchasing/Warehousing – Niagara	Enterprise Shared Services	Operational/Financial	11/10/14
11	FIN14600	Purchasing/Warehousing – St. Lawrence	Enterprise Shared Services	Operational/Financial	11/10/14
12	OPR14090	Social Media Governance	Enterprise Shared Services	Operational/Financial	11/10/14
Fieldwork Complete – Report Pending Issuance: 10					
13	OPR14006	Northern Region O&M	Operations	Operational/Financial	
14	OPR14060	Enterprise Risk	Business Services	Operational/Financial	
15	FIN14627	Customer Revenues - Niagara	Business Services	Operational/Financial	
16	FIN14241	Western NY Economic Development Fund	Economic Development & Energy Efficiency	Operational/Financial	
17	IS014740	Cyber Security	Operations/Enterprise Shared Services	Information Technology	
18	IS014701	ITAC Process/IT Capital Projects	Enterprise Shared Services	Information Technology	
19	FIN14106	Generation Resource Management	Operations/Energy Resource Management	Operational/Financial	

Appendix B – 2014 IA Plan

Ref.	Audit #	Audit	Business Unit	Audit Type	Issuance Date
20	OPR14080	Employee Information Concerns Line	Law	Operational/Financial	
21	FIN14295	SENY Cost of Service/ Long Term Agreements	Business Services	Operational/Financial	
22	IS014217	Virus Protection & Response	Enterprise Shared Services	Information Technology	
Fieldwork In Progress: 8					
23	OPR14130	Succession Planning/Retention Programs	Enterprise Shared Services	Operational/Financial	
24	FIN14105	Energy Efficiency Operations – Built Smart NY	Economic Development & Energy Efficiency	Operational/Financial	
25	FIN14305	Energy Efficiency Projects – Statewide Program	Economic Development & Energy Efficiency	Operational/Financial	
26	OPR14002	Public Authorities Law Compliance	Law/Various	Operational/Financial	
27	IS014720	IT Incident Response Plan	Enterprise Shared Services	Information Technology	
28	IS014710	Infrastructure Virtualization	Enterprise Shared Services	Information Technology	
29	OPR14200	Power System Operations/Energy Control Center	Operations	Operational/Financial	
30	IS014760	General Controls over SCADA - Northern & Central	Enterprise Shared Services	Information Technology	
Audit Planning In Progress: 6					
31	OPR14050	Human Resources Operations	Enterprise Shared Services	Operational/Financial	
32	OPR14101	Headquarters Procurement	Enterprise Shared Services	Operational/Financial	
33	OPR14095	Energy Trading Process & Controls Assessment	Business Services	Operational/Financial	
34	OPR14111	Quality Assurance/Code Compliance	Operations	Operational/Financial	
35	IS014207	Mobile Device Security & Controls	Enterprise Shared Services	Information Technology	
36	IS014210	IT Disaster Recovery - Governance	Enterprise Shared	Information Technology	

Appendix B – 2014 IA Plan

Ref.	Audit #	Audit	Business Unit	Audit Type	Issuance Date
			Services		
Postponed - Moved to 2015 IA Plan: 3					
37	FIN14263	NYISO Energy Settlements – Generation	Operations	Operational/Financial	
38	FIN14260	Customer Load Forecasting	Economic Development & Energy Efficiency	Operational/Financial	
39	IS014750	Network ITGC Review - Security & Change Management	Enterprise Shared Services	Information Technology	

RESOLUTION

RESOLVED, That pursuant to the Audit Committee Charter adopted by the Authority on February 23, 2010, the Audit Committee recommends that the proposed 2015 Internal Audit Plan be approved.