



**NY Power  
Authority**

***Audit Committee Meeting  
Internal Audit Update and  
Proposed 2016 Audit Plan***

***12/17/2015***



## Table of Contents

---

- Executive Summary
- Status of Audit Recommendations
- Transformation Status
- Third Party Support
- 2016 Audit Plan Development Process

Appendix A – Proposed 2016 Audit Plan

Appendix B – 2015 IA Plan

Appendix C – 2016 Risk Assessment – Projects Considered but Not Included in Plan

## Executive Summary

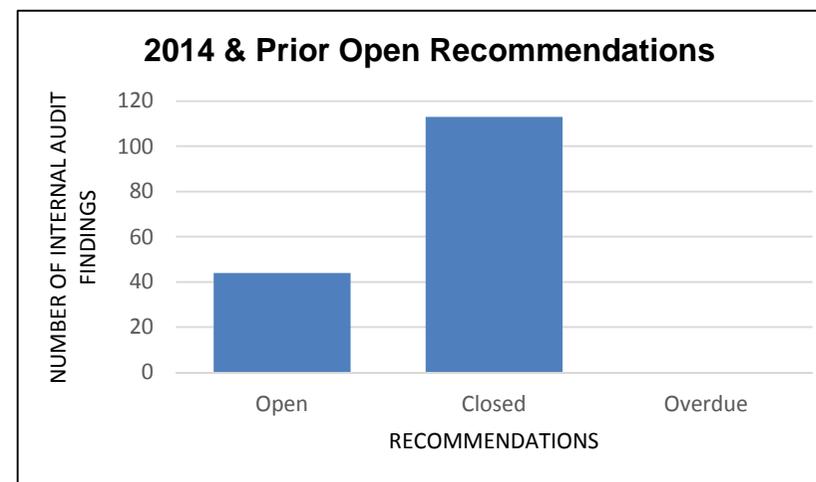
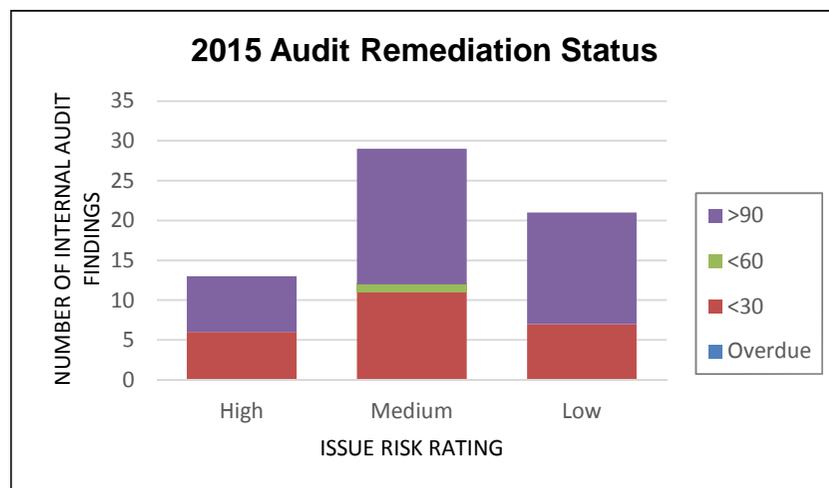
- 2015 Status: 20 of 31 audits have been issued as of 12/17/15. Seven (7) reports have been issued since 9/29/15.
- All fieldwork for the 2015 audit plan is estimated to be completed by December 31, 2015

2015 Internal Audit Report	Report Rating	
Physical Security – User Access Memo (OPR15900)	N/A	
Physical Security (OPR15900)	Satisfactory	
Licensing Operations (OPR15009)	Improvement Needed	
Budgeting and Forecasting (FIN15420)	Satisfactory	
User Access Management Process (IS015340)	Improvement Needed	
Asset Accounting/Maximo Post Implementation (IS015116)	Satisfactory	
NYPA Travel Expenses (FIN15115)	Satisfactory	

## Status of 2015 Audit Recommendations

- Below is the status of the 2015 recommendations per rating of the individual findings.
- A Project Team has been created to re-evaluate and formally update issues and recommendations prior to 2015.
- 72% of 2014 & Prior open recommendations have been completed.

2015 Remediation	Total	High	Medium	Low
At 9/29/15	50	15	22	13
Added in Period	26	4	12	10
Closed in Period	13	3	7	3
Open @ End of Period	63	16	27	20



\*As ratings have been established for 2015 reports onwards, recommendations prior to 2015 do not include risk ranking for recommendations.

# Transformation Status

People	
Activity	Status
Staffing	●
Hired: 12	
Open: 4	
Creation of on-boarding program	●
Training and development program creation	●
NERC CIP V5 Training	
Work-paper Documentation Training	
Develop guest auditor program	●
Launch customer feedback evaluations	●
Develop learning plans /training programs supporting competency & career mapping	●
Update job descriptions and core competencies	●
Office Site Team Building Meeting	●

Other	
Activity	Status
Re-Branding	●
Lunch and Learns	
Fordham - Beta Alpha Site Presentation	
Networking	●
NYISO Market Participant Advisory Council	
NYSSCA Local Events	
Quarterly Meeting with local CAE of Peers	
Advanced Women Executive Network	
2016 IT & SME Co-Source Partner RFP	●

Process	
Activity	Status
Execute 2015 Plan	●
2016 Audit Plan Development	●
Design Risk Assessment Process	
Execute 2016 RA	
Develop 2016 Audit Plan	
Revise IA Charter	●
Develop department templates	●
Analytics	●
Design analytics program	
Pilot analytics program	
Launch analytics program	
Recommendation Status	●
Formalize Follow-up Process	
Review/Validate 2014 & earlier Recommendations	
Develop Quality Assurance Process	●

Technology	
Activity	Status
Toolset	●
Document requirements analysis	
Consult with Risk Alignment and Controls Committee	
Build FY16 budget for technology and tool enhancement	
Select toolset and procure/design customization	●
Conduct training and education on use of tool and pilot initial audits	●

Completed	On track	Not started	At risk	Will not complete
-----------	----------	-------------	---------	-------------------



## Third Party Support

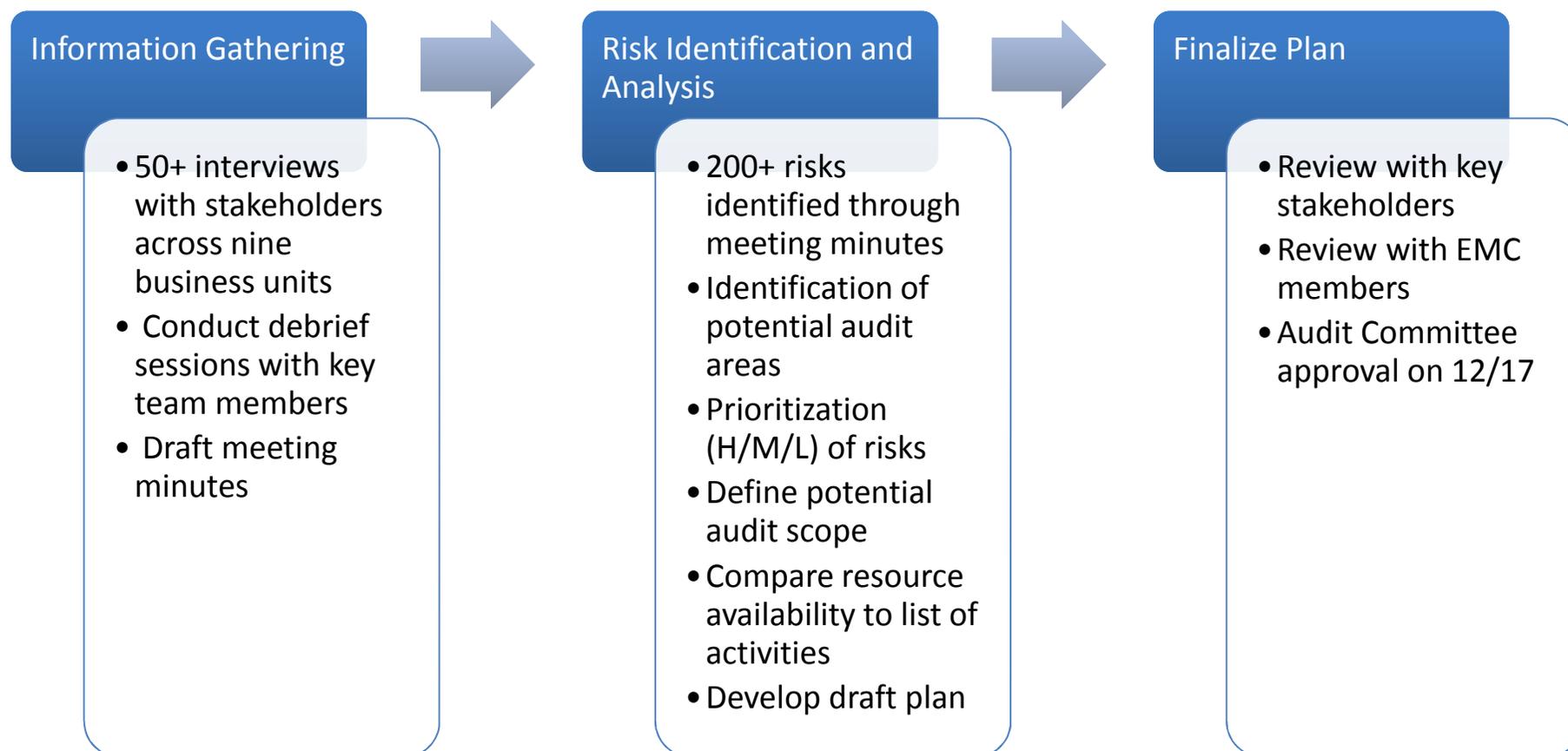
	2016*	2015
Cost	\$1.5M	\$4M
Scope of Services	Resources to support: <ul style="list-style-type: none"> <li>• 15 technology activities</li> <li>• 4 Subject matter resource activities</li> <li>• Limited project management support</li> </ul>	Resources to support: <ul style="list-style-type: none"> <li>• Completion of 2014 &amp; majority of 2015 audit plan (non-technology and technology)</li> <li>• Activity oversight by E&amp;Y management per their internal quality guidelines including partner peer review</li> <li>• Project management</li> <li>• Onboarding support/transition for new hires</li> </ul>
Activity Execution	All activities will be led by NYPA resources. Any consultants used will be responsible for documenting knowledge transfer	Until Q4, all activities were led and managed by E&Y resources. After IA hired permanent resources, activity management began to transfer to NYPA

### Request For Proposal (RFP) for 2016 Support

- RFP was released for review and response on November 23rd. Responses are required back by December 15<sup>th</sup>. Anticipated selection of a new vendor by February 28<sup>th</sup>.
- In interim between January 1<sup>st</sup> and selection of a new vendor, the E&Y scope of work will be extended to provide any technology and project management resources necessary.

\* Represents estimate included in 2016 budget

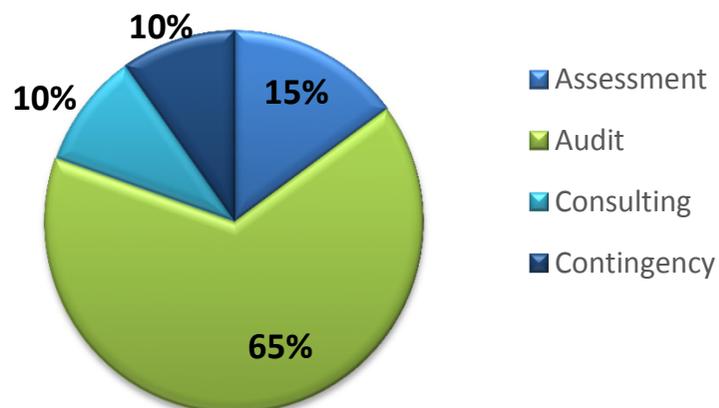
## 2016 Audit Plan Development Process



## 2016 Audit Plan – Activities & Time Allocation

### 2016 Planned Activities

- 54 projects in the Proposed 2016 Audit Plan:



### 2016 vs 2015

- Significant increase (74%) in planned activities:

	2016 Plan	2015 Actual
Assessments	9	1
Audits	33	25
Consulting	7	5
Contingency*	5	0
<b>Total</b>	<b>54</b>	<b>31</b>

### Activity Definitions

- Audit:** A look back - independent assessment of the performance of NYPA's risk management, control, and governance processes
- Assessment:** A look forward - advisory assessment, focused on process improvement opportunities, risk identification and mitigation within new processes or initiatives
- Consulting:** Ongoing - consulting and partnering arrangements that result in documented feedback or real time verbal feedback.
- Contingency:** Hours reserved for emerging risks (enterprise, fraud, etc.).

\* Contingency is an estimate and was calculated using the average hours for all planned projects.

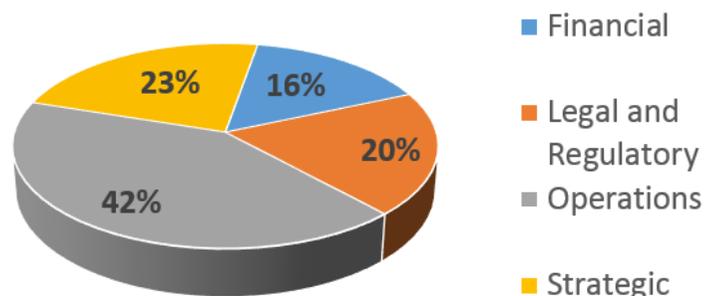
## 2016 Resource Allocation

*Resource Allocation: 54 projects are included based on resource availability*

Resource Allocation	Non-Technology	Technology
Actual Resource hours available <sup>a</sup>	15,900	0
Budgeted Third Party hours available <sup>b</sup>	350	4,300
<i>Proposed 2016 Audit Plan Hours</i>	<i>16,250</i>	<i>4,300</i>

### 2016 Planned Allocation

- Allocation by audit area <sup>c</sup>:



<sup>a</sup> Internal resource hours exclude time related to training/development, vacation, holiday, sick days, and administrative time. Additionally, this excludes the hours related to the 10% contingency.

<sup>b</sup> Third Party hours are based on unapproved budget allocation.

<sup>c</sup> Excludes projects that may arise from the 10% contingency.

### 2016 Draft Plan

- See Appendix A for draft plan
- See Appendix B for list of activities that will not be in scope for 2016
- The allocation of audit by area does not materially deviate from that proposed in the IA transformation program

# Appendix

# Appendix A – Proposed 2016 Audit Plan

#	Proposed Project	Activity Type	Business Unit	Risk(s)	Description/Preliminary Scope	Risk Category	Risk Rating	Timing
1	Customer Meter to Cash Audit	Audit	Economic Development & Energy Efficiency	Inaccurate or incomplete scheduling and/or settlement between NYISO, market participants, and NYPA's customers could lead to financial losses and/or incorrect customer bills.	Confirm that from the delivery of energy to NYPA's customer (at the meter), to the receipt of cash to satisfy accounts receivable, that NYPA is accurately allocating energy and other costs and billing/collecting those costs to/from its customers. Within this audit, we will consider both physical and financial transactions to the extent they exist. Processes and related handoffs between the following groups are in scope: Metering, Scheduling/Forecasting, Settlements, Energy Charge Adjustments and other rate related adjustments, Billing, Accounts Receivable/Collections, etc.	Financial	High	Q3
2	NERC CIPv5 Implementation Support (targeted assessments)	Consulting	Operations	Failure to comply with new NERC CIPv5 requirements may result in regulatory costs or increased regulatory scrutiny.	Targeted assessments during period 1/1/16 through 3/31/16 to ensure processes, procedures and controls are socialized and working as designed to support NYPA's CIPv5 compliance.	Legal and Regulatory	High	Q1
3	Ariba Post Implementation Review	Audit	Business Services	Delays in or an unexpected outcome when implementing Ariba could lead to inefficient or ineffective controls over the procurement process.	Conduct post implementation review activities of new Ariba modules as they are being planned for and released.	Operations	High	Q3 & Q4
4	End User Computing - Spreadsheets	Assessment	Entity-Wide	Overreliance on spreadsheets in decision making could lead to suboptimal decisions and decisions that are informed with inconsistent or inaccurate information.	Conduct an assessment of the current and potential future state for governing, monitoring and protecting critical spreadsheets for the organization.	Operations	High	Q1
5	Occupational Health & Safety Program Audit	Audit	Operations	Lack of safety culture could lead to injury or loss of life.	Evaluate program level governance and controls including monitoring provided by centralized EH&S Department on safety related matters for both management and bargaining unit employees. Ensure trends/themes from independent third party auditor are being identified by centralized EH&S and incorporated into NYPA's program.	Legal and Regulatory	High	Q2
6	BG SCADA - Pre/Post Implementation Review	Audit	Operations	Delays in or unexpected outcome of BG SCADA upgrade could result in negative impact to plant operations.	Conduct pre & post implementation review activities to ensure BG SCADA upgrade is completed on-time, within budget and without defects.	Operations	High	Q4
7	Vendor Management Governance Assessment	Assessment	Entity-Wide	Poor vendor, service provider, consultant or contractor performance could lead to inefficiencies within NYPA, confusion or conflict with our customers, performance delays or quality deficiencies, litigation against NYPA or impairment to NYPA's reputation.	Evaluate current vendor management (vendors, services providers, contractors and consultants) practices across NYPA including organizational governance and assess need/opportunity for entity-wide vendor management approach.	Operations	High	Q2

## Appendix A – Proposed 2016 Audit Plan

#	Proposed Project	Activity Type	Business Unit	Risk(s)	Description/Preliminary Scope	Risk Category	Risk Rating	Timing
8	Program Change Management Review	Audit	Technology & Innovation	The lack of adequate change management processes and controls with proper segregation of duties may increase the risk of unauthorized changes implemented to production environment, inconsistency, and inefficiency from the operations and supporting personnel.	Evaluate the technology change management process and governance organization wide in IT and OT including the policies and procedures, ownership of the processes and controls, documentation requirements, and segregation of duties between development and production environment. Test select high risk controls based on the understanding of the design of the processes and controls.	Operations	High	Q4
9	Strategic Plan Governance - Follow-up	Audit	Business Services	Lack of organizational support and alignment could lead to NYPA not achieving its strategic objectives.	Conduct a follow-up audit to validate the implementation of previous audit recommendation and to test the effectiveness of controls designed to provide transparency into the identification and mitigation of strategic initiative implementation related risks.	Strategic	High	Q3
10	Transmission O&M Audit	Audit	Operations	Ineffective maintenance practices may impact operational performance.	O&M Audit - confirm the following: - cross-functional assessment of Transmission and Generation O&M activities - newly created Maximo utilization procedures are consistently followed - monitoring of work activities is conducted - maintenance completion consistent with work prioritization methodology - root cause assessment (TapRoot) of equipment or system failure is conducted and followed up on.	Operations	High	Q2
11	Targeted Network Review	Assessment	Technology & Innovation	Failure to establish and maintain a robust network security configuration and restrict high privileged accounts to appropriate individuals without conflicting roles may increase the risk of exposure to vulnerability.	Review the managed network (encryption, security, segmentation), authentication (TACACS), network logging, redundancy, firewall filtering policies, clear text service protocols, and change management processes.	Operations	High	Q2
12	Workforce Planning Strategic Initiative Support	Consulting	HR & Enterprise Shared Services	Unclear or ineffective governance over the Workforce Planning Strategic Initiative may result in the organization not achieving its strategic objectives	IA to be embedded in the workforce planning initiative to ensure controls related to the alignment of workforce to company needs is adequate.	Strategic	High	Ongoing
13	Technical Training Audit	Audit	Operations	Critical skills shortages could lead to an increasing number of errors or delays in completing normal business activities, project delays or deficiencies, increased outages, increased safety violations, etc.	Ensure adequacy and effectiveness of technical training activities (including the Apprenticeship Program) including design and delivery of training to meet key skills requirements at NYPA. Assess internal and external constraints which may negatively impact technical training.	Operations	High	Q4

## Appendix A – Proposed 2016 Audit Plan

#	Proposed Project	Activity Type	Business Unit	Risk(s)	Description/Preliminary Scope	Risk Category	Risk Rating	Timing
14	Product and Service Marketing Assessment	Assessment	Economic Development & Energy Efficiency	Lack of customer awareness of NYPA products and services could lead to unrecoverable investments in new products/services and the inability for NYPA to achieve its strategic objectives.	Evaluate the following in support of the CES strategic initiative: - response/actions planned from the Strategic Initiative's marketing study - accuracy and completeness of marketing materials developed to inform existing and potential new customers of NYPA's product/service offerings - methods by which marketing information is made available to customers - methods by which management is monitoring/controlling the success of its marketing efforts - methods by which NYPA is monitoring changing customer preferences	Strategic	High	Q1
15	NERC Reliability Compliance Controls Audit(s)	Assessment	Operations	Non compliance with reliability compliance standards may result in significant fines and increased regulatory scrutiny.	Evaluate NYPA's Integrated Risk Assessment and Internal Control Evaluation activities and the role of IA in supporting the long-term objectives of these initiatives. Where appropriate, conduct targeted assessments to confirm the effectiveness of internal controls as identified by management in their Internal Controls Evaluation.	Legal and Regulatory	High	Q3
16	CES Technology Solution Support	Consulting	Economic Development & Energy Efficiency	Unclear requirements for potential new CES system may impact the achievement of business objectives.	Conduct pre/post implementation review activities for new CES systems being developed and/or implemented.	Strategic	High	Ongoing
17	Project Management Cycle Audit	Audit	Operations	Inefficient or ineffective project management activities could result in suboptimal use of resources and projects that do not meet objectives.	Ensure adequacy and effectiveness of controls throughout the project management life cycle including but not limited to project initiation and approval (including CEAR, new project evaluation metrics such as ROI and EVA, etc.), planning, controlling, execution, and closeout and the related handoffs between functional departments.	Operations	High	Q3
18	Cloud Governance	Assessment	Entity-Wide	Increasing reliance on cloud based technology solutions could result in changing O&M costs and the associated implications to the pass through of costs to customers, changing cyber security profile for NYPA, etc.	Assess the need for and options for NYPA to develop consistent governance of, contract requirements and other key controls when contemplating/deploying cloud based solutions.	Strategic	High	Q1

## Appendix A – Proposed 2016 Audit Plan

#	Proposed Project	Activity Type	Business Unit	Risk(s)	Description/Preliminary Scope	Risk Category	Risk Rating	Timing
19	Strategic Asset Management Plan Support	Consulting	Operations	Unclear or ineffective governance over the Asset Management Strategic Initiative may result in the organization not achieving its strategic objectives	IA to be embedded into the strategic initiative as a key stakeholder to provide independent and objective support in the design of internal controls. In addition, work during this consulting project will include determining opportunities for IA to support NYPA in its pursuit of ISO 55000.	Strategic	High	Ongoing
20	Patch Management Review	Audit	Technology & Innovation	The lack of adequate patch management processes and controls may increase the risk of unauthorized changes implemented to production environment, inconsistency, and inefficiency from the operations and supporting personnel to manage the latest version or patch implementation.	Evaluate the patch management process and governance including how necessary patches are identified, authorized, tested, and approved for implementation. Select and test the current patch compliance levels within IT and OT on a sample basis.	Operations	High	Q2
21	Sustainability Assessment	Assessment	Entity-Wide	The mismanagement of "socially responsible" activities may result in an unfavorable corporate perception with stakeholders, customers, suppliers, business partners, employees and the regulatory community.	Evaluate the need/opportunity for enhanced/continued governance of sustainability related activities at NYPA. Perform an analysis of current processes in place to obtain and be informed of all sustainability regulations, and apply them throughout NYPA. Assess whether key regulations have not been considered and whether employees are complying with sustainability requirements.	Legal and Regulatory	High	Q3
22	User Access Recertification Review at OS, DB Network Layers	Audit	Technology & Innovation	Failure to periodically review and recertify high privileged user access at the infrastructure and network systems may result in unauthorized access to sensitive/ critical data and changes via user access that is not needed or not authorized.	Review the design of IT & OT periodic user access recertification process/ controls at network, application, database, and operating system focusing on high privileged accounts (HPA).	Operations	High	Q3
23	Succession Planning	Assessment	Entity-Wide	Significant workforce retirements or an increasing number of staff exiting NYPA could lead to knowledge loss and critical skills shortages.	Conduct an assessment of the organization, governance and tools related to succession planning activities across NYPA and provide recommendations for improving activities to meet NYPA strategic plan objectives.	Strategic	High	Q2
24	De-provisioning Review	Audit	Technology & Innovation	Failure to remove terminated or transferred users' access from systems and/ or network increase the risk of unauthorized access to the systems, records in those systems, and company network.	Perform a review of the design of the user access de-provisioning process and controls within the numerous IT/OT systems including network, applications, databases, and operating systems. The in-scope systems for this review will be based on how the user authentication (user ID and/ or password) are managed (i.e. single sign-on, using the same ID/password of active directory).	Operations	High	Q3

## Appendix A – Proposed 2016 Audit Plan

#	Proposed Project	Activity Type	Business Unit	Risk(s)	Description/Preliminary Scope	Risk Category	Risk Rating	Timing
25	Lock-Out/Tag-Out Compliance Audit	Audit	Operations	Ineffective lock out/tag out of energized equipment could lead to an employee safety incident or an unplanned outage.	Ensure NYPA personnel continue to rigorously follow the requirements in CPP1 related to lock out and tag out. Ensure PTR system and related interfaces continue to enable the effective implementation of CPP1.	Operations	High	Q2
26	Generation Bidding Audit	Audit	Wholesale Commercial Operations	Lack of a clear operating strategy for generating assets could result in unexpected losses to NYPA or excessive cycling of the plant that leads to increased outages.	Ensure generation bid strategies exist and are being executed to optimize the value of NYPA's generation assets. NOTE: emphasis for the audit will be on Flynn (new merchant unit), SCPPs and BG	Operations	High	Q1
27	Fuel Purchasing & Hedging Audit	Audit	Wholesale Commercial Operations	Increasing or unexpected changes in natural gas commodity prices could result NYPA's fossil generating assets to be uneconomical.	Ensure controls over the purchase of fuel are adequate and working effectively to minimize the cost of fuel and ensure adequate supply to optimize the value of NYPA's generating assets.	Operations	High	Q2
28	Performance Management Audit (Level 1, Business Unit, Department and Individual)	Audit	Business Services	Lack of corporate objectives and performance metrics could result in conflicts as to how line and business unit management prioritize work activities.	Ensure the socialization of corporate performance measures and the alignment of the measures to business unit, department and individual employee performance goals/expectations as appropriate.	Strategic	High	Q4
29	Northern NY Power Proceeds Audit	Audit	Economic Development & Energy Efficiency	Noncompliance with the Northern NY Power Proceeds program could significantly impact designated communities and impair NYPA's reputation.	Ensure adequacy and effectiveness of controls in place to comply with the Northern NY Power Proceeds program/agreement.	Legal and Regulatory	High	Q4
30	Cyber Security Rollup / Consolidation	Assessment	Entity-Wide	Duplicative and/or redundant efforts may be in progress due to multiple technology consultant engagements producing overlapping management recommendations.	NYPA Management has engaged many (over ten) third parties to provide assessments of the technology control environment (including Cyber Security) in the last few years. Each engagement has identified numerous issues and produced a variety of recommendations. Based on this work, management has developed multiple action plans which are in various stages of completion. Internal Audit will review the recommendations and actions plans and "level set" / prioritize them against each other in order to provide management with a single set of prioritized actions that management can consider implementing.	Operations	Medium	Ongoing
31	Data Analytics Initiatives Support	Consulting	Entity-Wide	Lack of clear definition of and objectives for Data Analytics could lead to unnecessary investments and the inability for NYPA to achieve its strategic plan.	IA to be embedded in NYPA IT Strategic Plan - Data Analytics Initiative as well as other entity-wide initiatives such as the Asset Management Strategic Initiative focused on Data Analytical to provide internal control and other enterprise level support.	Strategic	High	Ongoing

## Appendix A – Proposed 2016 Audit Plan

#	Proposed Project	Activity Type	Business Unit	Risk(s)	Description/Preliminary Scope	Risk Category	Risk Rating	Timing
32	Transmission LEM Project Audit	Audit	Operations	Inefficient or ineffective project management activities could result in suboptimal use of resources and projects that do not meet objectives.	Large Construction Project Audit - ensure project risks are being identified and mitigated, project is conducted consistent with CEAR/approval, that management is aware of the projects status and that significant vendors or contractors are performing in accordance with contract terms.	Operations	High	Q3
33	Contract Governance and Control Audit	Audit	Entity-Wide	New/Changing contracts for products and services may not adequately protect NYPA's interests that could lead to unanticipated litigation outcomes or NYPA's inability to meet customer expectations and operations.	Confirm NYPA has consistent governance and control over new and changing contracts (ad hoc or standardized). Processes to be considered include contract development, negotiation, review, approval and filing/retention. Additionally, we will confirm the clarity of roles and responsibilities within the individual processes and where handoffs between processes exist.	Legal and Regulatory	High	Q2
34	Affordable Care Act Compliance Assessment	Consulting	HR & Enterprise Shared Services	The new Affordable Care Act could result in significant benefits cost increases to NYPA (via Cadillac Tax) or NYPA's workforce.	IA to be embedded in management's evaluation process over the various compensation and benefits being offered that could affect NYPA being subject to the Affordable Care Act Cadillac tax. These activities include but are not limited to a review of current benefits providers and the associated contract bidding process planned for 2016 as well as a review and potential re-write of employees policies.	Legal and Regulatory	High	Q3
35	Western Region O&M Audit	Audit	Operations	Ineffective maintenance practices may impact operational performance.	O&M Audit - confirm the following: - newly created Maximo utilization procedures are consistently followed - monitoring of work activities is conducted - maintenance is completed consistent with work prioritization methodology - root cause assessment (TapRoot) of equipment or system failure is conducted and followed up on.	Operations	High	Q1
36	Contractor Tenure	Audit	Entity-Wide	Failure to identify and prevent legal risks posed by contractors and prevent non-compliance with state/local and country specific regulatory requirements; Failure to onboard workers appropriately to ensure adequate knowledge transfer.	Assess the current process, policies and procedures in place for utilizing contractors and for complying with Department of Labor requirements.	Legal and Regulatory	High	Q4
37	Muni/Coop Regulation Audit	Audit	Economic Development & Energy Efficiency	New/changing business requirements for municipal and cooperative customers could result in increased litigation, external stakeholder influence and impaired reputation to NYPA.	Ensure NYPA's regulation of full requirements and monitoring/oversight of partial requirements municipal and cooperative is adequate and effective.	Legal and Regulatory	High	Q3
38	Energy Efficiency Finance & Accounting	Audit	Economic Development & Energy Efficiency	Misaligned business activities could lead to inaccurate financial information informing business decisions	Evaluate the adequacy and effectiveness of controls within the Economic Development & Energy Efficiency Business Unit's finance and accounting function. Assess the consistency of activities to corporate finance and accounting governance expectations.	Financial	High	Q2

## Appendix A – Proposed 2016 Audit Plan

#	Proposed Project	Activity Type	Business Unit	Risk(s)	Description/Preliminary Scope	Risk Category	Risk Rating	Timing
39	Past Due Receivables Audit	Audit	Business Services	Customer payment defaults could result in NYPA writing off uncollectable receivables.	Evaluate the adequacy and effectiveness of controls to ensure a consistent and measured response by NYPA to past due receivables to minimize default risk.	Financial	Medium	Q2
40	Payroll Cycle Audit	Audit	Business Services	Ineffective or inefficient payroll processing activities could result in incorrect, improper or unauthorized payments to employees.	Confirm the adequacy and effectiveness of controls over payroll processing including but not limited to timekeeping, master file updates, policy enforcement, exceptions, processing and approvals for various payroll related activities including Flex, overtime and other payroll related exceptions.	Financial	Medium	Q1
41	R&D Spend Audit	Audit	Technology & Innovation	Lack of clear R&D objectives or inability to achieve objectives could result in suboptimal R&D spending and/or negative external stakeholder perception of NYPA.	Ensure controls are adequate and working effectively to ensure R&D spend is consistent with R&D objectives.	Strategic	Medium	Q1
42	Vegetation Management Vendor Audit	Audit	Operations	Lack of oversight of vegetation management contractor could lead to excessive costs or poor performance.	Ensure adequacy and effectiveness of vendor management controls to ensure quality of vendor performance and management of costs.	Operations	Medium	Q1
43	St. Lawrence - Finance & Administration Audit	Audit	Operations	Misaligned administrative processes within the region could lead to inefficiencies or ineffective control over financial and human resources.	Ensure adequacy and effectiveness of finance and administration activities at the site including but not limited to recruiting and performance management, financial discipline (budgeting and expense management, financial acumen), T&E, etc.	Financial	Medium	Q2
44	Energy Commodity Risk Management GAP Analysis Support	Consulting	Risk Management	Failure to effectively understand the mitigate energy commodity risks could lead to unexpected impacts to NYPA's financial performance.	IA to be embedded in the project to evaluate energy commodity risk management at NYPA and resolve gaps between current and potential future state strategies. The project will lead to potential changes in processes and tools for managing energy commodity risks.	Strategic	High	Ongoing
45	Clark Energy Center - Finance & Administration Audit	Audit	Operations	Misaligned administrative processes within the region could lead to inefficiencies or ineffective control over financial and human resources.	Ensure adequacy and effectiveness of finance and administration activities at the site including but not limited to recruiting and performance management, financial discipline (budgeting and expense management, financial acumen), T&E, etc.	Financial	Medium	Q3

## Appendix A – Proposed 2016 Audit Plan

#	Proposed Project	Activity Type	Business Unit	Risk(s)	Description/Preliminary Scope	Risk Category	Risk Rating	Timing
46	SENY - Purchasing & Warehousing Audit	Audit	Operations	Failure to procure and maintain necessary equipment necessary to operate equipment/systems due to inadequate asset management planning, incorrect or obsolete materials in stock, inventory stock-out, and/or delays in procurement.	Ensure consistent application of controls for the purchase of goods and materials at the site and the effective management of inventory to meet the plant's operational needs.	Financial	Medium	Q3
47	Concur (travel & entertainment expense) Pre/Post Implementation Review	Audit	Business Services	Delays in or an unexpected outcome when implementing Concur would result in a continuation of a recognized inefficient T&E process (links to Process Excellence strategic initiative) and employee dissatisfaction.	Conduct Pre/Post implementation review activities for new travel & entertainment (T&E) expense processing software.	Operations	High	Ongoing
48	Customer Job Audits (D&M)	Audit	Economic Development & Energy Efficiency	Noncompliance with Recharge NY and other power allocation program (EP, RP, etc.) legislation could lead to increased regulatory scrutiny and negative impact to NYPA's reputation.	Recurring audit support for NYPA Marketing Department to support compliance program.	Legal and Regulatory	Medium	Q2 and Q4
49	Third Party Contract Audits	Audit	Entity-Wide	Third party vendor nonperformance could lead to delays or failure to achieve business objectives, impairment of NYPA's reputation or increased litigation.	Identify high risk third party contracts (vendor, service provider, contractors or consultants) and exercise our audits rights to confirm performance in accordance with contract terms including accuracy of invoicing and contract deliverables.	Operations	High	Ongoing

## Appendix B – 2015 IA Plan

Ref.	Audit #	Audit	Business Unit	Audit Type	Date Issued
<b>Deliverable Issued: 20</b>					
1	IS015380	IT Project Management Office (PMO)	Enterprise Shared Services	Audit	5-13-15
2	FIN15440	Strategic Plan Governance and Execution	Business Services	Consultative	5-21-15
3	FIN15400	Compensation & Benefits	Enterprise Shared Services	Audit	6-04-15
4	IS015320	Cyber Security - Network Discovery	Enterprise Shared Services	Audit	6-09-15
5	OPR15140	Fleet Operations	Enterprise Shared Services	Audit	6-10-15
6	FIN15450	Cost Accounting Study	Business Services	Consultative	6-12-15
7	IS015390	Records Management	Enterprise Shared Services	Audit	6-26-15
8	OPR15220	Construction Projects	Business Services	Audit	7-10-15
9	OPR15260	Fraud Awareness Risk Assessment	Law Department	Consultative	7-16-15
10	IS015310	Cyber Security - Maturity Assessment with IT	Enterprise Shared Services	Audit	7-16-15
11	FIN15900	Niagara Finance & Accounting	Business Services	Audit	7-16-15
12	CON15001	First Energy Cost Validation	Law Department	Audit	7-30-15
13	OPR15230	O&M Cross Functionality	Operations	Consultative	9-16-15
14	OPR15900	Physical Security – User Access Memo	Operations	Audit	10-6-15
15	OPR15900	Physical Security	Operations	Audit	10-27-15
16	OPR15009	Licensing Operations	Public & Regulatory Affairs	Audit	10-27-15
17	FIN15420	Budgeting and Forecasting	Business Services	Audit	11-6-15
18	IS015340	User Access Management Process	Enterprise Shared Services	Audit	11-18-15
19	IS015116	Asset Accounting/Maximo Post Implementation	Enterprise Shared Services	Audit	11-18-15
20	FIN15115	Travel & Entertainment	Enterprise Shared Services	Audit	12-8-15
<b>Fieldwork Complete – Report Pending Issuance: 3</b>					
21	FIN15460	Disposal of Personal Property	Economic Development & Efficiency	Audit	
22	IS015350	High Value Asset Identification (Data Loss Prevention)	Enterprise Shared Services	Audit	
23	FIN15251	Purchasing/Warehousing – BG	Business Services	Audit	

## Appendix B – 2015 IA Plan

Fieldwork In Progress: 6					
24	OPR15250	FERC Dam Safety	Operations	Audit	
25	OPR15003	NERC CIP Initiatives	Operations	Audit	
26	OPR15280	Customer Compliance	Economic Development & Efficiency	Audit	
27	IS015410	Enterprise Architecture Review	Enterprise Shared Services	Consultative	
28	OPR15290	Compliance Submissions	Law Department	Audit	
29	OPR15270	Supplier Diversity Program Assessment	Business Services	Audit	
Audit Planning In Progress: 1					
30	OPR15310	Job Pooling	Business Services//Human Resources	Consultative	

## Appendix C - 2016 Risk Assessment – Projects Considered but Not Included in Plan

#	Proposed Project	Description/Preliminary Scope	Action
1	Generator Meter to Cash Audit	Confirm that from the delivery of energy from NYPA's generators to the grid (at the meter) to the receipt of cash to satisfy accounts receivable that NYPA is accurately accounting for and settling energy and ancillary services with individual customers or market participants. Processes and related handoffs between the following groups are in scope: Metering, Generation Bidding, NYISO Settlements, Billing, etc.	Generation Bid in 2016 - will conduct end to end meter to cash in 2017.
2	BuildSmart NY (EO88) Audit	Follow-up audit to ensure controls related to the BuildSmart NY Program remain adequate and ensure compliance with new requirements/mandates of EO88 since prior audit.	2014 audit work - delay additional work to future period
3	Compliance Reporting Audit	Verify that required compliance reporting is accurate and on-time. NOTE: Use Denise Baker database for initial repository for sampling.	2015 audit work - integrate into individual 2016 audits.
4	Environmental Compliance Audit	Evaluate program level governance and controls including monitoring provided by centralized EH&S Department on environmental compliance matters. Ensure trends/themes from independent third party auditor are being identified by centralized EH&S and incorporated into NYPA's program.	Another 3d LOD exists - monitor their activities only.

## Appendix C - 2016 Risk Assessment – Projects Considered but Not Included in Plan

#	Proposed Project	Description/Preliminary Scope	Action
5	Compliance Training Audit	Verify that required compliance training is being delivered to impacted personnel (timing and content). NOTE: Use Denise Baker database for initial repository for sampling.	Audit of Technical Training in 2016. Integrate into individual 2016 audits.
6	HTP Operations Audit	Ensure controls in place to manage the operations and maintenance of the HTP line are adequate and working effectively including: <ul style="list-style-type: none"> <li>- compliance with policies and procedures</li> <li>- oversight of line operations vendor (ConEd Solutions)</li> <li>- transparency in performance to assist management in long-term decision-making.</li> </ul>	Audited in 2015; consulting support for governance materials build in 2015
7	Wheeling Expense Audit	Evaluate the adequacy and effectiveness of controls to ensure the accuracy of wheeling charges and the proper allocation of costs to customers.	for 2016 - emphasis on Meter to Cash
8	Contributions and Sponsorships Compliance Audit	Confirm NYPA has up-to-date procedures to comply with NYS contribution and sponsorship guidelines and that procedures are being consistently followed.	Rated as low risk.

## Appendix C - 2016 Risk Assessment – Projects Considered but Not Included in Plan

#	Proposed Project	Description/Preliminary Scope	Action
9	Success Factors Pre/Post Implementation Review	Conduct pre/post implementation reviews of various Success Factors modules as they are introduced to provide support in ensuring adequate controls are implemented.	IA involvement in workforce planning initiative will allow adequate coverage.
10	Talisen Contract Audit (NY Energy Manager)	Contract audit of Talisen to ensure controls are in place to monitor service provider performance and that service provider controls can be validated. NOTE: Ensure contract provisions are adequate to protect NYPA and our customer's data.	Utilization of services remains low - consider in 2017.
11	CIMS to Maximo Asset Data Migration Pre/Post Implementation Review	Conduct pre/post implementation review activities for the conversion of data and business process changes when migrating CIMS to Maximo.	Per Bruce - this will not happen in 2016
12	Procurement to Payment Cycle Audit	Review of procedures, process and controls across the various process that make up the procurement to payment cycle including but not limited to requisition, RFQ, bid review/selection, Purchase Order/contract award, contract management, vendor invoicing, accounts payable, treasury.	Significant change in business processes - audit in 2017

## Appendix C - 2016 Risk Assessment – Projects Considered but Not Included in Plan

#	Proposed Project	Description/Preliminary Scope	Action
13	Workforce Planning Process Excellence Project	IA to be an active participant including understanding current and desired future cycle times, developing of a job pooling methodology, etc.	Process Excellence is not scheduling this for 2016.
14	OT Asset Mgt Review. (physical verification)	Requirement under NERC - CIP-002.5: BES Cyber System Categorization While the 2015 Maximo audit looked at the system and processes, we did not cover physical verification. Review the effectiveness of an organization's existing asset reliability program and continuous maintenance activities. For high-risk critical assets, conduct a targeted reliability review to determine the likelihood and impact of a significant failure CIMS to Maximo: critical for BES assets	2017 plan - foundational.
15	OT Cyber Security Maturity Assessment (C2M2)	Requirement under NERC CIP-003-5: by requiring CIP Senior Management approval for policy related to each standard. Maturity Assessment for OT based on changes in the departments	2017 plan - foundational.
16	IT Asset Mgt Review	Perform completeness walkthrough by performing physical count and tying it back to the asset management systems at selected sites	2017 plan - foundational.

## Appendix C - 2016 Risk Assessment – Projects Considered but Not Included in Plan

#	Proposed Project	Description/Preliminary Scope	Action
17	Post-implementation review of OT Interactive Remote Access	Conduct a post-implementation review of the interactive remote access initiative (framework, technology, implementation).	2017 plan - foundational.
18	OT Data Loss Prevention (DLP) Controls	Evaluate the adequacy and effectiveness of data loss prevention tools and methodology.	2017 plan - foundational.
19	nMarket - Shadow Settlements Solution Support	Provide support to Economic Development as they evaluate and determine the best solution for conducting shadow settlements.	will participate but not formal project for IA.
20	Enterprise Emergency Management, Disaster Recovery/Backup, Business Continuation and Incident Response Review	IA to be embedded with the Emergency Management audit issue mitigation project to develop and implement an enterprise framework for Emergency Management, Disaster Recovery, Business Continuity, Incident Response and Crisis Management.	will participate but not formal project for IA.

## Appendix B - 2016 Risk Assessment – Projects Considered but Not Included in Plan

#	Proposed Project	Description/Preliminary Scope	Action
17	Post-implementation review of OT Interactive Remote Access	Conduct a post-implementation review of the interactive remote access initiative (framework, technology, implementation).	2017 plan - foundational.
18	OT Data Loss Prevention (DLP) Controls	Evaluate the adequacy and effectiveness of data loss prevention tools and methodology.	2017 plan - foundational.
19	nMarket - Shadow Settlements Solution Support	Provide support to Economic Development as they evaluate and determine the best solution for conducting shadow settlements.	will participate but not formal project for IA.
20	Enterprise Emergency Management, Disaster Recovery/Backup, Business Continuation and Incident Response Review	IA to be embedded with the Emergency Management audit issue mitigation project to develop and implement an enterprise framework for Emergency Management, Disaster Recovery, Business Continuity, Incident Response and Crisis Management.	will participate but not formal project for IA.

## Appendix C - 2016 Risk Assessment – Projects Considered but Not Included in Plan

#	Proposed Project	Description/Preliminary Scope	Action
21	Primavera Pre/Post Implementation Review	Conduct post implementation review of Primavera conversion (from inhouse to Cloud) to ensure accuracy and completeness of data conversion and socialization of new processes across Energy Efficiency.	IA involvement in CES initiatives will allow monitoring in 2016.
22	Clark Energy Center - Purchasing & Warehousing Audit	Ensure consistent application of controls for the purchase of goods and materials at the site and the effective management of inventory to meet the plant's operational needs.	cycle audit - conduct in 2017
23	LPGP LEM Project Audit	Large Construction Project Audit - ensure project risks are being identified and mitigated, project is conducted consistent with CEAR/approval, that management is aware of the projects status and that significant vendors or contractors are performing in accordance with contract terms.	cycle audit - conduct in 2017