Questions received on DASNY IT Audit & Advisory Services and DASNY's responses:

1) Is the total value of the Contract limited to $50,000 per year? Or is the above just 1 parameter in the overall context of the contract award?

Response:

The contract awarded will be a zero-dollar contract with the anticipation of issuing work authorizations for IT audit and advisory services on an as needed basis, subject to available funding. Based on current planning assumptions, annual expenditure is expected to be approximately $50,000, but actual usage may vary and could increase during the contract term.

2) What is the total US dollar value of the 5-year contract to be awarded? Is there a specific budget we must be aware of?

Response:

The contract awarded will be a zero-dollar contract with the anticipation of issuing work authorizations for IT audit and advisory services on an as needed basis, subject to available funding. Based on current planning assumptions, annual expenditure is expected to be approximately $50,000, but actual usage may vary and could increase during the contract term.

3) Is this a brand-new contract or an extension of an existing contract? If existing, what is the current contract #?

Response:

This is a brand-new contract.

4) For IT, what are the positions/titles that our firm must include for DASNY in the Cost Proposal Form? Currently, the XLS is blank, hence asking.

Response:

The positions, titles, and certifications of those individuals who will be working with the Internal Audit function for the audit and advisory work should be provided.

5) Multiplier of 2.5 or less mentioned, could you please explain what DASNY's allowed / unallowed items are so we can calculate appropriately?

Response:

DASNY allows a multiplier of 2.5 or less without financial statement verification. If requesting a higher multiplier, financial statements will need to be provided, and we will review direct and indirect costs to support the requested multiplier.

6) Could you provide more details on the current scope and methodology of DASNY's existing IT risk assessment that requires updating and validation?

Response:

An IT risk assessment was completed in 2022 using the Information Technology Infrastructure (ITIL) framework. The assessment identified approximately 55 IT functional areas across the ITIL lifecycle domains, including Service Strategy, Service Design, Service Transition, and Service Operations. The IT assessment focused on evaluating the different IT functional areas within DASNY based on their alignment to and impact on enterprise-level risks. Since completion of the assessment, some changes have occurred within DASNY's technology systems and IT operating landscape. As a result, the assessment requires review, validation, and updating to reflect current conditions, emerging risks, and priorities.

7) Are there any specific frameworks (e.g., NIST, ISO 27001) or regulatory compliance standards (e.g., PCI DSS, HIPAA, GLBA) that DASNY prioritizes for the IT risk assessment and audit plan?

Response:

No. Previous IT audit activities generally reference recognized frameworks and standards, including the NIST Cybersecurity Framework and ISO-based practices, as appropriate, to inform risk identification and prioritization. These frameworks are used as guidance rather than as prescriptive compliance requirements. Where applicable, regulatory or compliance considerations may be addressed within the scope of individual audits based on the nature of the systems, data, or services under review. The Internal Audit function is open to recommendations that align with leading practices and the organization's risk profile.

8) Is there a preferred format or template for the detailed IT risk assessment and the five-year proposed audit plan to be delivered?

Response:

No, there is not a preferred format or template. However, it should be consistent with applicable professional standards, including the IIA Global Internal Audit Standards.

9) How can we obtain the full Request for Proposal (RFP) documents or any supplementary information related to this bid?

Response:

The documents can be found on DASNY's website at www.dasny.org / Opportunities / RFPs & Bids / Professional Services / IT Audit & Advisory Services / View the full details for this opportunity / Attachments.

10. What major IT platforms and environments are in scope (e.g., ERP, cloud, custom systems)?

Response:

The IT risk assessment and audit activities should consider all major enterprise systems and technology platforms in scope. Examples include enterprise applications (e.g. ERP systems

such as Microsoft Dynamics), project management systems, cloud services, and other organizational technology platforms, based on risk and organizational priorities.

11. Are there regulatory drivers influencing IT risk (e.g., NYS cybersecurity, privacy statutes)?

Response:

There are no specific regulatory drivers that mandate or directly influence the IT risk assessment or audit plan.

12. How mature is the current IT risk assessment (recent, outdated, informal)?

Response:

An IT risk assessment was completed in 2022 using the Information Technology Infrastructure (ITIL) framework. The assessment, completed by internal audit staff in conjunction with IT staff, identified approximately 55 IT functional areas across the ITIL lifecycle domains, including Service Strategy, Service Design, Service Transition, and Service Operations. The IT assessment focused on evaluating the different IT functional areas within DASNY based on their alignment to and impact on enterprise-level risks. Since completion of the assessment, changes have occurred within DASNY's technology environment, systems, and IT operating landscape. As a result, the assessment requires review, validation, and updating to reflect current conditions, emerging risks, and priorities.

13. Does DASNY expect the 5-year plan to align with enterprise risk management (ERM) outputs?

Response:

The IT risk assessment and audit plan should consider IT functional areas in the context of DASNY's objectives and enterprise risks, including operational, strategic, IT, legal and compliance, and financial risks.

14. Are certain IT domains pre-identified as high priority (IAM, cloud, third-party risk, SDLC)?

Response:

No.

15. Is there an expectation to map risks/audits to specific frameworks (NIST CSF, 800-53, etc.)?

Response:

In the past the IT audits generally referenced recognized frameworks and standards, including the NIST Cybersecurity Framework and ISO-based practices, as appropriate, to inform risk identification and prioritization. These frameworks are used as guidance rather than as prescriptive compliance requirements. Internal Audit is open to recommendations that align with leading practices and DASNY's risk profile.

16. What level of hands-on execution vs. advisory oversight does Internal Audit expect?

Response:

A hybrid approach to IT audit support is expected. The selected audit firm should anticipate providing hands-on execution for one IT audit annually, while also providing advisory and audit oversight support for an additional one to two IT audits conducted by internal staff. This should be a co-sourcing model.

17. How many DASNY IA staff will typically participate in each engagement?

Response:

Two; one Senior Internal Auditor and the Director of Internal Audit.

18. What documentation standards or audit tools do Internal Audit currently use?

Response:

The Internal Audit department follows the Institute of Internal Auditors (IIA) Global Internal Audit Standards and currently uses Microsoft tools (Word, Excel, etc.).

19. Historically, how has DASNY allocated similar annual audit/advisory budgets?

Response:

Similar to the current budget.

20. Should the $50,000 annual cap be modeled as: One large audit? Multiple smaller audits? Audit + advisory mix?

Response:

The selected audit firm should anticipate providing hands-on execution for approximately one IT audit annually, while also providing advisory and oversight support for an additional one to two IT audits performed by internal audit staff.

21. Who is the primary audience for IT audit reports (Audit Committee, executive leadership)?

Response:

The primary audience for IT audit reports include the Audit Committee, executive leadership, and IT management.

22. Are executive-level summaries or dashboards expected?

Response:

Executive summaries within individual audit reports should be provided, but dashboards are not expected.

23. Are there preferred report formats or templates?

Response:

The Internal Audit department maintains standard reporting formats and templates for audit and risk assessment activities. However, alternative formats or templates may be proposed, provided they meet reporting requirements and are consistent with applicable professional standards, including the IIA Global Internal Audit Standards.

24. Does DASNY anticipate the same lead personnel across the full contract term?

Response:

No, the same lead is not required. However, continuity and familiarity with DASNY's IT environment, processes, and prior assessments is highly valued to ensure effective and efficient oversight.

25. Are subcontractors permitted, and if so, under what conditions?

Response:

This Contract does not allow for sub-contracting opportunities.

26. Does DASNY maintain a formal IT asset inventory/system register that will be the starting point for the IT risk assessment?

Response:

The previously completed IT risk assessment, which outlines the IT functional areas and processes, will be provided as a reference. In addition, an application and system register will be made available to help inform the risk assessment.

27. Should the IT risk assessment include: Third-party hosted systems (SaaS, PaaS)? Vendors managed by other DASNY departments?

Response:

Yes. The IT risk assessment should consider third-party hosted systems and vendor-managed systems, including those managed by other departments. Such systems should be evaluated based on their relevance to DASNY's IT environment and risk profile.

28. Are OT systems, facilities systems, or construction-related technologies in scope or out of scope?

Response:

In scope.

29. Is DASNY expecting inherent and residual risk scoring, or a single composite risk score?

Response:

The methodology for assessing risk should be based on a framework that establishes criteria for risk rating using qualitative and quantitative factors which are clearly defined.

30. Are there any known "must-include" risk areas that Internal Audit or the Audit Committee already expects to see addressed?

Response:

No, not necessarily.

31. Is DASNY seeking alignment to a specific NIST framework (e.g., CSF vs. 800-53), or is framework selection left to the firm?

Response:

An IT risk assessment was completed in 2022 using the Information Technology Infrastructure (ITIL) framework. In the past, IT audits completed generally referenced recognized frameworks and standards, including the NIST Cybersecurity Framework and ISO-based practices, as appropriate, to inform risk identification and prioritization. These frameworks are used as guidance rather than as prescriptive compliance requirements. The Internal Audit function is open to recommendations that align with leading practices and DASNY's IT risk profile.

32. Does Internal Audit already use: An IIA-aligned audit methodology? A standard risk rating scale that must be reused.

Response:

The Internal Audit function follows the IIA Global Internal Audit Standards. Alternative rating scales may be proposed, provided they meet reporting requirements and are consistent with applicable professional standards, such as the IIA Global Internal Audit Standards.

33. Are there existing IA templates (risk registers, audit reports, scoring models) that the firm must adopt?

Response:

The Internal Audit function maintains standard reporting formats and templates for audit and risk assessment activities. However, alternative formats or templates may be proposed, provided they meet reporting requirements and are consistent with applicable professional standards, including the IIA Global Internal Audit Standards.

34. Will IT audit reports be presented directly to the Audit Committee, or only through Internal Audit?

Response:

The selected firm should anticipate presenting the results of IT audit reports to IT management only.

35. Is there an expectation for: Executive summaries? Heat maps? Trend analysis across years?

Response:

An executive summary should be included within individual audit reports, but there is not expectation for heat maps or trend analysis.

36. Does the Audit Committee have specific recurring IT concerns (cybersecurity, data privacy, resilience)?

Response:

No.

37. Historically, how has DASNY used similar not-to-exceed advisory budgets?

Response:

We use an NTE (not to exceed) type budget when the scope may evolve but staying within the budget is critical. When we make assignments, we will ask the awarded vendor to provide an estimated cost using their approved hourly rates and anticipated number of hours to complete a task.

38. Should firms assume: One large audit per year? Multiple targeted audits? Audit + advisory hybrid?

Response:

A hybrid approach to IT audit and advisory support should be assumed. The selected audit firm should anticipate providing hands-on execution for one major audit annually, while also providing advisory and oversight support for an additional one to two IT audits conducted by internal audit staff.

39. Is unused budget forfeited annually, or can work be shifted across years?

Response:

The Internal Audit function is funded on an annual fiscal year basis (April 1 through March 31). Services are expected to be completed within the applicable fiscal year, and any unused budget is not typically carried forward.

40. Are advisory services expected to be reactive (on-call) or pre-planned?

Response:

Advisory services are expected to include both preplanned and on-call components. The selected firm should anticipate providing scheduled advisory support aligned with planned audits, while also offering on-demand guidance and oversight for any emerging risks or ad hoc requests.

41. Is DASNY expecting the same engagement lead throughout the full contract term?

Response:

No, the same lead is not required. However, continuity and familiarity with DASNY's IT environment, processes, and prior assessments is highly valued to ensure effective and efficient oversight.

42. Are subcontractors or subject-matter specialists permitted?

Response:

This Contract does not allow for sub-contracting opportunities.

43. If subcontractors are allowed: Must they meet the same certification requirements? Must they be disclosed at proposal time?

Response:

N/A.

44. Who retains ownership of audit workpapers?

Response:

DASNY's Internal Audit function retains ownership of all audit work papers. The selected firm is expected to provide all work papers and supporting documentation to the Internal Audit function upon completion of the engagements or as requested.

45. Are workpapers subject to FOIL requests?

Response:

As a public entity in New York State, organizational records may be subject to disclosure under applicable public records laws. Internal Audit workpapers are evaluated in accordance with Freedom of Information requirements and applicable exemptions.

46. Is there an expectation that workpapers be stored in: DASNY systems? The firm's systems?

Response:

The selected firm is expected to provide all work papers and supporting documentation to the Internal Audit function for storage within DASNY's systems upon completion of the engagements or as requested.

47. What level of quality assurance review does Internal Audit expect prior to report issuance?

Response:

It is expected that all audit and advisory deliverables will undergo internal quality assurance review by the Internal Audit function prior to final report issuance. The review ensures accuracy, completeness, and adherence to applicable professional standards.

48. Has DASNY historically received FOIL requests for: IT audit reports? Risk assessments?

Response:

No.

49. Are there preferred methods for marking sensitive or exempt content?

Response:

No preferred methods. If applicable, it will be discussed.

50. Will DASNY support redaction requests where appropriate?

Response:

Yes, if appropriate.

51. Is there a page limit or formatting requirement for the technical proposal?

Response:

No, there is not a page limit or formatting requirement.

52. Will pricing be evaluated independently or weighed up with qualifications?

Response:

Pricing will be weighted along with qualifications and proposal content as part of the overall evaluation.

53. Does DASNY anticipate awarding to: One firm? Multiple firms for different work streams?

Response:

It is anticipated that one firm will be awarded a contract.

54. Will clarification responses become binding addenda?

Response:

Yes, if submitted through the RFI process. All questions and answers will be posted as an addendum to the Procurement.

55. How does DASNY define a "successful" IT audit engagement?

Response:

A successful IT audit engagement is one that effectively assesses IT risks, evaluates key controls, and provides actional findings and recommendations, while maintaining close coordination with the Internal Audit function throughout the engagement.

56. What pain points has DASNY experienced with prior co-sourced IT audit arrangements?

Response:

DASNY has not encountered notable issues with prior IT audit or advisory arrangements.

57. What would DASNY want to see improved or done differently this time?

Response:

The Internal Audit function continually seeks opportunities to improve its IT audit and advisory practices. For example, staff training and development to enhance IT knowledge and expertise is an area of ongoing focus.

58. Does DASNY anticipate all Phases of the Engagement to be completed remotely?

Response:

Yes, all phases of the engagement can be completed remotely.

59. What access and support would be available?

Response:

The selected firm will have the support of the Internal Audit function and may collaborate with the IT department as needed. Access to relevant systems, documentation, and staff will be provided to the extent necessary to perform audit and advisory activities.

60. Has DASNY previously outsourced this function?

Response:

No.

61. Has DASNY previously completed an IT audit, IT-related risk assessment?

Response:

An IT risk assessment was completed in 2022 using the Information Technology Infrastructure (ITIL) framework. The Internal Audit function completes IT audits annually.

62. Will the documentation from any prior external or internal IT audits be available for review?

Response:

Yes, as appropriate.

63. If an audit was performed, when was the last audit?

Response:

The Internal Audit function typically conducts IT audits on an annual basis.

64. What is DASNY's budget for Phase 1 – Development of an IT Risk Assessment and 5-Year IT Audit Plan?

Response:

Phase One, which includes the development or update of the IT Risk Assessment and audit plan, will be funded from the current fiscal year IT audit and advisory services budget. If Phase

One extends into the next fiscal year (April 1 – March 31), costs will be covered under the following year's IT audit and advisory services budget.

65. Which systems or tools does DASNY use for daily operations including financial, accounting, HR, other systems?

Response:

DASNY uses a variety of IT systems to support daily operations, including financial, HR, and project management functions. Representative systems include Microsoft Dynamics 365, a project management system, and other applications supporting operational and administrative functions.

66. Is the infrastructure on premise, cloud based, or hybrid?

Response:

Hybrid.

67. If cloud based, what platform is DASNY using (M365, Google, etc).

Response:

M365.

68. How many concurrent users does DASNY have across the IT landscape?

Response:

Concurrent users include internal employees (500+) and authorized third party users who have access to applicable IT systems. The number of concurrent users varies by system and application.

69. How many people make up DASNY's Internal Audit function?

Response:

There are five people in the Internal Audit Department: a Director, an Assistant Director, two Senior Internal Auditors, and an Internal Auditor.

70. Does DASNY currently have governance or oversight committees in place related to IT risk?

Response:

Yes.

71. Is DASNY's IT support internal or has it been outsourced?

Response:

Internal.

72. If outsourced, what functions do the outsourced IT cover?

Response:

N/A.

73. What is the total number of applications, databases, and network segments included in the IT universe for the Phase 1 risk assessment? (RFP section 2.1)

Response:

An IT risk assessment was completed in 2022 using the Information Technology Infrastructure (ITIL) framework. The assessment identified approximately 55 IT functional areas across the ITIL lifecycle domains, which serve as the foundation for defining the IT universe.

DASNY has two domains, a parent and child, with an estimated 470 active users and approximately 200 applications.

74. What percentage of the IT infrastructure is hosted in the cloud (e.g., Azure, AWS) versus on-premises data centers?

Response:

The organization operates a hybrid IT environment consisting of both cloud-hosted and on-premise infrastructure. Cloud services support a significant portion of enterprise applications, while certain systems and data remain hosted within on-premise environments.

75. How many distinct physical locations or satellite offices fall within the scope of the IT audit plan?

Response:

The IT audit plan should primarily focus on core IT operations and infrastructure, with consideration of field locations as they relate to the IT systems and critical controls. While DASNY has multiple construction field sites, only those facilities (3 offices) supporting key IT systems and processes are expected to be generally included within the audit scope.

76. Does the IT universe include Operational Technology (OT) or Industrial Control Systems (ICS) related to facility management?

Response:

Yes, the IT universe includes operational technology and industrial control systems supporting facility management, such as building systems/

77. Which specific NIST SP 800-53 control baseline (Low, Moderate, or High) is DASNY currently utilizing, or is the expectation to use the NIST Cybersecurity Framework (CSF)? (RFP section 2.3)

Response:

An IT risk assessment was completed in 2022 using the Information Technology Infrastructure (ITIL) framework. In the past, IT audits completed generally referenced recognized

frameworks and standards, including the NIST Cybersecurity Framework and ISO-based practices, as appropriate, to inform risk identification and prioritization. These frameworks are used as guidance rather than as prescriptive compliance requirements. The Internal Audit function is open to recommendations that align with leading practices and DASNY's IT risk profile.

78. Are there specific regulatory requirements beyond New York State standards, such as CJIS, HIPAA, or PCI-DSS, that must be included in the risk assessment?

Response:

No.

79. To what degree of granularity must the five-year audit plan define "audit hours" for future years - at the control level or the functional area level?

Response:

The five-year audit plan should include total estimated audit hours only for engagements expected to require external expertise and be performed by the selected firm over the next three to five years.

80. What is the expected frequency of status meetings and formal presentations to the Audit Committee?

Response:

The firm selected will not be expected to provide formal presentations to the Audit Committee. Status meetings with Internal Audit should occur weekly during ongoing engagements, as applicable.

81. Will DASNY provide a dedicated project management tool for workpaper sharing, or is the consultant expected to provide a secure audit platform?

Response:

The firm selected is expected to provide a secure audit platform.

82. What is the anticipated percentage of "on call/technical advisory support" hours expected annually within the $50,000 cap?

Response:

A hybrid approach to IT audit support is expected. The selected audit firm should anticipate providing hands-on execution for one IT audit annually, along with technical advisory and oversight support for an additional one to two IT audits performed by internal staff. On-call hours are expected to represent a minimum portion of total hours annually, less than 1%.

83. How many Internal Audit staff members will be assigned to the co-sourced team for Phase 2 audits?

Response:

One Senior Internal Auditor and the Director of Internal Audit will be included within IT audits.

84. What is the current maturity level of existing IT documentation (e.g., recent SOC reports, previous risk assessments, or system security plans)?

Response:

An IT risk assessment was completed in 2022 using the Information Technology Infrastructure (ITIL) framework. The assessment, completed by internal audit staff in conjunction with IT staff, identified approximately 55 IT functional areas across the ITIL lifecycle domains, including Service Strategy, Service Design, Service Transition, and Service Operations. The IT assessment focused on evaluating the different IT functional areas within DASNY based on their alignment to and impact on enterprise-level risks. Since completion of the assessment, changes have occurred within DASNY's technology environment, systems, and IT operating landscape. As a result, the assessment requires review, validation, and updating to reflect current conditions, emerging risks, and priorities.

85. Are there specific blackout dates or "busy seasons" for DASNY IT personnel that would impact the Phase 1 development schedule?

Response:

No.

86. Does DASNY require or prefer any reference contacts to be included in our proposal?

Response:

No.

87. Section 2.2 - What specific audit management activities do you expect the firm to own vs. Internal Audit to own (audit coordination, scheduling, requests, presentation to management/Audit Committee, follow-up validation)?

Response:

Presentations to the Audit Committee will go through the internal audit function only and not the selected firm. For audit coordination, the proposed approach is that the external IT firm would own coordination for the audits they perform, while Internal Audit would manage the coordination for audits conducted inhouse.

88. Section 2.4 - Does DASNY have preferred audit software/workpaper tools, templates, or reporting formats we must use (or should we supply our own)?

Response:

The Internal Audit department maintains standard reporting formats and templates for audit and risk assessment activities and utilizes Microsoft word and excel for audit workpapers. However, alternative formats or templates may be proposed, provided they meet reporting requirements and are consistent with applicable professional standards, including the IIA Global Internal Audit Standards.

The firm selected is expected to provide a secure platform for sharing audit documents.

89. Section 2.1 - Is DASNY comfortable sharing the existing IT risk assessment referenced in the RFP and when it was last updated?

Response:

An IT risk assessment was completed in 2022 using the Information Technology Infrastructure (ITIL) framework. This will be provided to the selected firm as a starting point for the IT risk assessment.

90. Section 2.1 - Is there a target completion date for Phase 1 deliverables and a planned Audit Committee meeting when the plan will be presented/approved?

Response:

Yes, the target completion for phase one is March 31, 2026. The plan will be presented to the Audit Committee by Internal Audit in mid-April 2026.

91. Section 3 - Should we assume fully remote delivery, or include periodic onsite meetings? If onsite is needed, what locations and frequency?

Response:

The selected firm should plan full remote delivery.

92. Section 2.1: How does the "risk assessment support" noted in Phase 3 relate to the Risk Assessment work noted in Phase 1?

Response:

Phase one establishes the enterprise IT risk universe and risk priorities. Phase three support applies this framework by providing technical advisory and oversight assistance for IT audits performed by internal audit staff, including guidance on risk evaluation and audit approach.

93. Section 2.1: Have the services being requested in the RFP been provided by another firm prior to this RFP? Or has it traditionally been handled in house by the Internal Audit?

Response:

The requested services have historically been delivered through a hybrid approach. External firms have been engaged for specialized technical IT audits requiring specific expertise, while other risk assessment and audit activities have been performed in-house by internal audit staff.

94. Section 2.1: Phase 2, historically, what types of audits have traditionally been outsourced?

Response:

Examples of recent IT audits that have been outsourced include Active Directory, Network Segmentation, and Cloud Security.

95. Section 2.1: What is the expectation of on-site work vs. the firms working remotely?

Response:

The firm is expected to work 100% remote.

96. Section 2.1: Phase 3, historically, what types of IT advisory services have been performed?

Response:

IT audit services have been performed externally; however, IT advisory services have not historically been performed. The internal audit function is seeking these services to enhance internal capabilities by obtaining specialized technical guidance, risk advisory support, and subject matter expertise to support IT risk assessment and audit activities.

97. Can DASNY briefly describe the types of IT systems, either enterprise or personal use, that might be considered in scope for audit and advisory services?

Response:

All enterprise IT systems and applications will be considered in scope for audit and advisory services based off the results of the phase one risk assessment.

98. In section 2.4 Other Technical Requirements, will DASNY staff working on co-sourced audit activities be located on-site at a DASNY location, remote, or hybrid?

Response:

Internal audit staff will be available 100% remote.

99. In section 2.1 - Phase 3 IT Advisory Services, can DASNY provide examples of advisory engagements typically requested (e.g., system implementation reviews, policy updates, cloud migration assessments)?

Response:

IT advisory services will include, for example, providing oversight and review of internal IT audits performed by internal audit staff, and providing technical expertise and engagement oversight without performing the hands-on execution of the audits performed in house by internal audit staff.

100. In section 2.1 - Phase 3 IT Advisory Services, what response-time expectation does DASNY have for "on-call" advisory requests?

Response:

On-call advisory services are expected to be infrequent and will be requested on an as-needed basis. The selected firm should respond in a reasonable timeframe consistent with the nature and urgency of the request.

101. (Section 2: Engagement Requirements, Paragraph 2 (Phase 1): Does DASNY have an existing IT risk assessment or prior IT audit plan we'd be updating, or would this be built from scratch?

Response:

An IT risk assessment was completed in 2022 using the Information Technology Infrastructure (ITIL) framework. The assessment identified approximately 55 IT functional areas across the ITIL lifecycle domains, including Service Strategy, Service Design, Service Transition, and Service Operations. The IT assessment focused on evaluating the different IT functional areas within DASNY based on their alignment to and impact on enterprise-level risks. Since completion of the assessment, some changes have occurred within DASNY's technology systems and IT operating landscape. As a result, the assessment requires review, validation, and updating to reflect current conditions, emerging risks, and priorities.

102. (Section 2: Engagement Requirements, Paragraph 2 (Phase 1): How many stakeholders/departments need to be interviewed during the risk assessment?

Response:

There is one IT department with 3-4 stakeholders that will be able to provide the information necessary for the IT risk assessment.

103. (Section 2: Engagement Requirements, Paragraph 2 (Phase 1): Does DASNY have a preferred risk assessment framework? Or will the awarded firm pick one?

Response:

In the past the IT audits generally referenced recognized frameworks and standards, including the NIST Cybersecurity Framework and ISO-based practices, as appropriate, to inform risk identification and prioritization. These frameworks are used as guidance rather than as prescriptive compliance requirements. Internal Audit is open to recommendations that align with leading practices and DASNY's risk profile.

104. (Section 2: Engagement Requirements, Paragraph 3 (Phase 2): For remote testing and auditing, will a VPN be provided for remote access? If not, then what method will be utilized?

Response:

Yes, remote access capabilities will be coordinated with the IT department as applicable.

105. (Section 2: Engagement Requirements, Paragraph 5 (Phase 3): For advisory services, is there an expected ratio of audit vs. advisory hours, or is this fully flexible?

Response:

A hybrid approach to IT audit support is expected. The selected audit firm should anticipate providing hands-on execution for one IT audit annually, while also providing advisory and audit oversight support for an additional one to two IT audits conducted by internal staff. This should be a co-sourcing model.

106. (Section 3: Content of Proposal, Paragraph 8.a): Does the $50K cap include expenses (travel, tools), or is that fee only?

Response:

The $50k should include all expected expenses.

107. (Section 3: Content of Proposal, Paragraph 8.a): Within the $50K annual cap, does DASNY have a sense of how many systems audits per year it anticipates (e.g., 1–2 full audits vs. several smaller reviews)?

Response:

A hybrid approach to IT audit support is expected. The selected audit firm should anticipate providing hands-on execution for one IT audit annually, while also providing advisory and audit oversight support for an additional one to two IT audits conducted by internal staff. This should be a co-sourcing model.

108. (Section 3: Content of Proposal, Paragraph 8.a): Is Phase 1 priced as a fixed fee or time-and-materials?

Response:

The pricing proposal can be provided as either a fixed fee or time-and-materials (based on hourly rates submitted).

109. (Section 3: Content of Proposal, Paragraph 8.a): Is the $50K annual not-to-exceed for Phases 2 & 3 a firm ceiling, or could it be supplemented for larger engagements?

Response:

Yes, the $50k is the not-to-exceed amount. A hybrid approach to IT audit support is expected. The selected audit firm should anticipate providing hands-on execution for one IT audit annually, while also providing advisory and audit oversight support for an additional one to two IT audits conducted by internal staff. This should be a co-sourcing model.

110. (Section 3: Content of Proposal, Paragraph 10): What multiplier has DASNY typically approved for similar professional services contracts?

Response:

Firms may request a 2.5 multiplier without providing financial statements. If a higher multiplier is required, firms must submit FARS audited financials.

111. Does DASNY have a defined budget for the Risk Assessment Development and Initial Audit?

Response:

Phase One, which includes the development or update of the IT Risk Assessment and audit plan, will be funded from the current fiscal year IT audit and advisory services budget of $50k. If Phase One extends into the next fiscal year (April 1 – March 31), costs for the risk assessment and audits will be covered under the following year's IT audit and advisory services budget of $50k.

112. Are we to assess risk within all IT Controls, Policies, and Procedures?

Response:

Risk should be assessed within IT controls, policies and procedures as applicable to the areas under review.

113. How large is the DASNY environment both internally and externally in terms of Hosts (IP Addressing), IP Subnetting, Remote Sites, and Data Centers to be tested?

Response:

DASNY has two domains, a parent and child, with an estimated 500 active users and approximately 200 applications. Areas for testing will be based off the results of the phase one risk assessment.

114. Can everything be tested from one main site?

Response:

Most testing, if not all, should be able to be performed remotely.

115. Is Testing to be done in White Box, Gray Box, or Black Box Mode?

Response:

The mode of testing will be determined based on the scope and objectives of each engagement. Testing methodology will be aligned with the type of system, the assessed risk, and the level of internal access required to effectively evaluate controls.

116. Is Web Application penetration testing in scope for Web Applications?

Response:

This will be based off the results of the IT risk assessment.

117. How many Web Applications are to be penetration tested?

Response:

This will be dependent upon the results of the IT risk assessment.

118. Can Testing be done On-site and Remotely during normal business hours?

Response:

Yes, as appropriate. If certain testing should be performed outside normal business hours to avoid network disruption, this can be coordinated with IT staff.

119. How many Servers and Virtualized Servers are in Scope for Testing?

Response:

This will be dependent upon the results of the IT risk assessment.

120. How many IT Personnel will be interviewed for conformance to IT Policy and Procedures?

Response:

This will be dependent on the IT area identified for audit.

121. How many Internal Auditors are there for Interview Purposes regarding IT Control Policy and Procedures?

Response:

One senior internal auditor and the Director of Internal Audit will be available on a co-sourcing basis.

122. What Framework does DASNY utilize to assess Compliance and or identify Gaps? (HIPAA, NIST CSF, NIST SP800-53 Rev. 5, CIS, GLBA)

Response:

In the past the IT audits generally referenced recognized frameworks and standards, including the NIST Cybersecurity Framework and ISO-based practices, as appropriate, to inform risk identification and prioritization. These frameworks are used as guidance rather than as prescriptive compliance requirements. Internal Audit is open to recommendations that align with leading practices and DASNY's risk profile.

123. Will DASNY provide the selected firm with access to both the current IT risk assessment and any prior IT audit plans at the outset of Phase 1? If so, in what format will these documents be provided, and will there be an opportunity to discuss their context with Internal Audit or IT leadership? *Reference: Page 3, Section 2.1*

Response:

Yes, these documents can be provided in an excel format and should be discussed with both Internal Audit and IT leadership.

124. Can DASNY provide an estimate or range for the number of core business applications, infrastructure platforms (on-prem/cloud), and critical vendors/third-party systems to be included in the IT risk assessment? *Reference: Not directly addressed in RFP.*

Response:

There are approximately 200 applications, however only approximately 10% of them are core business applications.

125. Does DASNY have a preferred risk scoring template or model, or should proposers submit a sample methodology aligned to IIA and NIST for review and approval? *Reference: Page 3, Section 2.1.*

Response:

The Internal Audit function follows the IIA Global Internal Audit Standards. Alternative risk rating scales may be proposed, provided they meet reporting requirements and are consistent with applicable professional standards, such as the IIA Global Internal Audit Standards.

126. Beyond risk ratings, audit frequency, and estimated hours per engagement, does DASNY expect the five-year IT audit plan to identify "quick-win" versus more complex audits, or should this be left to the firm's professional judgment? *Reference: Page 3, Section 2.1*

Response:

This should be left to the firm's professional judgment.

127. Are there any IT risk domains (e.g., cybersecurity, disaster recovery, vendor risk) that DASNY expects to prioritize in the upcoming risk assessment or audit plan? *Reference: Not directly addressed in RFP.*

Response:

At this time, no specific IT risk domains have been identified for prioritization. The audit plan will be developed using a risk-based approach, with areas of focus determined through the risk assessment process and alignment with organizational priorities.

128. Can DASNY provide examples or typical scopes of IT audits completed in recent years to help proposers calibrate approach and assumptions? *Reference: Not directly addressed in RFP.*

Response:

Examples of recent IT audit scopes that have been outsourced include Active Directory, Network Segmentation, and Cloud Security.

129. Will the selected firm act as lead auditor for individual IT audits, or primarily in a supporting/co-sourcing role to Internal Audit? *Reference: Page 4, Section 2.2.*

Response:

Both, the selected firm will act as lead auditor for approximately one IT audit a year that requires IT expertise and then act in a supporting/co-sourcing role for an additional IT audit performed by the internal audit function.

130. Does Internal Audit require the use of specific audit tools, workpaper systems, or report formats, or may the selected firm use its own preferred tools and templates? *Reference: Page 4, Section 2.2.*

Response:

The Internal Audit department maintains standard reporting formats and templates for audit and risk assessment activities and utilizes Microsoft word and excel for audit workpapers. However, alternative formats or templates may be proposed, provided they meet reporting requirements and are consistent with applicable professional standards, including the IIA Global Internal Audit Standards.

131. Does DASNY have a minimum expectation for the number or type of audits to be completed annually within the $50,000 cap, or should proposers define a recommended mix based on their experience? *Reference: Page 6, Section 3, Item 8a.*

Response:

A hybrid approach to IT audit support is expected. The selected audit firm should anticipate providing hands-on execution for one IT audit annually, along with co-sourcing support for an additional one to two IT audits performed by internal staff. A recommended mix based on their experience can also be proposed and would be considered.

132. What types of advisory activities does DASNY anticipate most frequently (e.g., remediation validation, control design review, framework alignment, technical consultation)? *Reference: Page 3, Section 2.1.*

Response:

All of the above, and workpaper review for IT audits performed by internal audit staff as applicable.

133. Should advisory services be assumed to consume hours from the same $50,000 annual cap as audit services? *Reference: Page 6, Section 3, Item 8a.*

Response:

Yes.

134. Does DASNY have a preferred approach for day-to-day coordination (e.g., frequency of status calls, use of shared project plans, formal review checkpoints), or should the firm propose a recommended structure? *Reference: Page 4, Section 2.2.*

Response:

No preferred approach. Yes, the firm should propose a recommended structure.

135. Will the selected firm present results directly to executive management or the Audit Committee, or will all communication flow through Internal Audit? *Reference: Page 4, Section 2.2.*

Response:

All communication will flow through the Internal Audit. The firm selected will not present results to executive management or the Audit Committee.

136. Should proposers assume all phases can be delivered remotely, or are there mandatory onsite requirements for any phase or audit engagement? *Reference: Page 4, Section 2.4.*

Response:

Yes, all phases can be delivered remotely.

137. Are there any specific onboarding, background check, or security clearance requirements for contractor staff engaged under this contract? *Reference: Not directly addressed in RFP.*

Response:

A Vendor Responsibility Review will be conducted prior to award.

138. Should firms assume timely access to DASNY personnel, documentation, and system walkthroughs for Phase 1 pricing purposes? *Reference: Page 5, Section 3, Item 6b.*

Response:

Yes.

139. Should proposers include anticipated travel costs in their pricing, or will travel be reimbursed separately if required? *Reference: Not directly addressed in RFP.*

Response:

All of the work should be able to be completed remotely. However, if travel were to be required, it should be included in anticipated travel costs in pricing.

140. Is DASNY open to considering optional add-on services, such as annual IT risk assessment refreshes or periodic audit plan recalibration, as part of the proposal? *Reference: Not directly addressed in RFP.*

Response:

Yes.

141. Section 2, Phase 1 - The service request seems to suggest the development of an IT risk assessment using a methodology, but then indicates the scope is to review, validate and update an existing IT risk assessment. Is DASNY looking for the service provider to perform a new risk assessment, update an existing risk assessment, or both?

Response:

An IT risk assessment was completed in 2022 using the Information Technology Infrastructure (ITIL) framework. The assessment, completed by internal audit staff in conjunction with IT staff, identified approximately 55 IT functional areas across the ITIL lifecycle domains, including Service Strategy, Service Design, Service Transition, and Service Operations. The IT assessment focused on evaluating the different IT functional areas within DASNY based on

their alignment to and impact on enterprise-level risks. Since completion of the assessment, changes have occurred within DASNY's technology environment, systems, and IT operating landscape. As a result, the assessment requires review, validation, and updating to reflect current conditions, emerging risks, and priorities.

142. Section 2, Phase 1 – Does DASNY follow a specific industry framework currently for completing its risk assessments?

Response:

The Internal Audit function follows the IIA Global Internal Audit Standards. Alternative frameworks may be proposed, provided they meet reporting requirements and are consistent with applicable professional standards, such as the IIA Global Internal Audit Standards.

143. Section 2, Phase 1 – The RFP suggests that DASNY has an existing IT universe that is determined and documented. Would the risk assessment be aimed toward assessing those defined elements?

Response:

An IT risk assessment was completed in 2022 using the Information Technology Infrastructure (ITIL) framework. The assessment, completed by internal audit staff in conjunction with IT staff, identified approximately 55 IT functional areas across the ITIL lifecycle domains, including Service Strategy, Service Design, Service Transition, and Service Operations. The IT assessment focused on evaluating the different IT functional areas within DASNY based on their alignment to and impact on enterprise-level risks. Since completion of the assessment, changes have occurred within DASNY's technology environment, systems, and IT operating landscape. As a result, the assessment requires review, validation, and updating to reflect current conditions, emerging risks, and priorities.

144. Section 2, Phase 1 vs Phase 2 - The audit plan deliverable produced in Phase 1 indicates that the scope of each audit needs to be defined with audit hours allocated to each engagement. However, Phase 2 indicates the focus is on defining the scope in a collaborative manner. Is the scoping and hours allocation performed in Phase 1 an estimate, and Phase 2 is more detailed scoping with IA pre audit?

Response:

Yes, that is correct.

145. Section 2, Phase 2 – Does DASNY aim to complete a specific number of IT audits annually? Approximately how many were conducted in the past two years?

Response:

The selected audit firm should anticipate providing hands-on execution for approximately one IT audit annually, while also providing advisory and oversight support for an additional one to two IT audits performed by internal audit staff.

Approximately three IT audits were conducted in the past two years.

146. Section 2, Phase 3 – Does DASNY have any historical estimate of the number of hours of advisory services that have been used in the past?

Response:

Advisory services have not been used in the past in this manner.

147. Section 2 – Can you clarify whether the risk assessment in Phase 1 will occur in year 1 only, or will this be performed / updated in future years as well?

Response:

The risk assessment will occur in year 1 only.

148. Section 3, part 7 vs 8 – The Phase 1 risk assessment is priced separately from Phases 2 and 3. If the expectation is for the service provider to perform / update the risk assessment in future years, should this be priced separately or as a portion of the annual cost allocation not to exceed $50,000 (e.g. advisory allocation)?

Response:

The risk assessment will only be performed in the first year.

149. Section 3, part 8 – Is DASNY open to having the service provider leverage a combination of qualified and experienced onshore and offshore resources to potentially accomplish a larger audit plan by leveraging less costly resources?

Response:

Offshore resources are not allowed under this contract.

150. What does the current IT landscape look like for DASNY?

Response:

An IT risk assessment was completed in 2022 using the Information Technology Infrastructure (ITIL) framework. The assessment, completed by internal audit staff in conjunction with IT staff, identified approximately 55 IT functional areas across the ITIL lifecycle domains, including Service Strategy, Service Design, Service Transition, and Service Operations. The IT assessment focused on evaluating the different IT functional areas within DASNY based on their alignment to and impact on enterprise-level risks. Since completion of the assessment, changes have occurred within DASNY's technology environment, systems, and IT operating landscape. As a result, the assessment requires review, validation, and updating to reflect current conditions, emerging risks, and priorities.

151. It looks like there is a cap of $50,000 a year for performing the work so how many audits would be anticipated to be performed on an annual basis from DASNY's perspective?

Response:

The selected audit firm should anticipate providing hands-on execution for approximately one IT audit annually, while also providing advisory and oversight support for an additional one to two IT audits performed by internal audit staff.

152. Are there any restrictions on access of data or evidence sharing we need to consider such as NYPA?

Response:

Yes, data sharing may be subject to organizational policies and security requirements.

153. Which frameworks or regulations matter most (e.g., NIST CSF/800-53, ISO 27001, CIS, PCI DSS, HIPAA, NYDFS) to DASNY?

Response:

Previous IT audit activities generally reference recognized frameworks and standards, including the NIST Cybersecurity Framework and ISO-based practices, as appropriate, to inform risk identification and prioritization. These frameworks are used as guidance rather than as prescriptive compliance requirements. Where applicable, regulatory or compliance considerations may be addressed within the scope of individual audits based on the nature of the systems, data, or services under review. The Internal Audit function is open to recommendations that align with leading practices and the organization's risk profile.

154. Related to the above, does DASNY follow a particular Cybersecurity framework (e.g., NIST CSF 2.0, NIST 800-53, ISO 27001, etc.) that any of the systems or infrastructure environments in-scope are required to be in compliance with from a controls standpoint?

Response:

Previous IT audit activities generally reference recognized frameworks and standards, including the NIST Cybersecurity Framework and ISO-based practices, as appropriate, to inform risk identification and prioritization. These frameworks are used as guidance rather than as prescriptive compliance requirements. Where applicable, regulatory or compliance considerations may be addressed within the scope of individual audits based on the nature of the systems, data, or services under review. The Internal Audit function is open to recommendations that align with leading practices and the organization's risk profile.

155. Do you have any expectations around the work being performed onsite vs. remote?

Response:

All work can be performed remotely.

156. Does DASNY currently utilize AI and would it potentially be one of the areas included in scope during the Risk Assessment (e.g., AI Governance)?

Response:

Yes, DASNY has a policy for organizational AI use, and yes it should be considered within the overall risk assessment.

157. In addition to your overall IT/Cybersecurity infrastructure, would the risk assessment process consist of a department by department look at the systems and technology utilized, to define potential systems to be included within the audit plan?

Response:

As part of the risk assessment process, a list of applications and systems will be provided, including the departments that utilize each system.

158. Does your Internal Audit Department currently have any type of audit software in place, that the selected vendor would need to use during the risk assessment and/or audit process?

Response:

No, the internal audit function does not use an audit software.

159. Would the use of offshore personnel be acceptable if they are employees of our firm and not subcontractors, and follow the same security protocols as our U.S. based employees

Response:

The use of offshore resources is not permitted for this contract.

160. Is there any budget allocated for this contract? If yes, can you please let us know the same?

Response:

There is a not to exceed budget of $50,000 per fiscal year (April 1- March 31)

161. Is there an incumbent on the contract? If yes, could you please let us know the incumbent name and spending done on the contract so far?

Response:

There is no incumbent.

162. What is the total number of resources the client is expecting to work on this project?

Response:

The total number of resources will be determined based on the scope, complexity, and timing of the audit work.

163. Are hourly rate ranges acceptable for the proposed personnel, including key personnel?

Response:

Yes, the hourly rate range for the proposed personnel, including key personnel, is acceptable.

164. Is the work entirely onsite, or can it be done remotely to some extent? Do the services have to be delivered onsite, or is there a possibility of remote operations and performance?

Response:

All work can be done remotely.

165. Are proposed staff resumes required along with the proposal? If yes, should they be live or sample resumes?

Response:

Yes, resumes are required for key personnel, and live resumes should be provided.

166. If a proposed key resource becomes unavailable, will a replacement with equal or greater qualifications be acceptable with the agency's approval?

Response:

Yes.

167. How many people are currently working onsite and offsite?

Response:

The number of onsite and offsite personnel will vary based on the scope and project requirements.

168. Could the client please clarify whether the post–vendor selection interview will be conducted in person or remotely?

Response:

If interviews are conducted, they will be done remotely.

169. Is subcontracting allowed for this project, and if so, are there any specific approval processes or qualifications required for subcontractors?

Response:

Subcontracting is not allowed for this type of contract.

170. Could you please share what ERP system is currently in use, and if there are any specific challenges or limitations you're experiencing with it?

Response:

ERP systems include Microsoft Dynamics, a project management system, cloud services, and other organizational technology platforms.

171. Does the agency currently utilize a Commercial Off-The-Shelf (COTS) ERP solution, or is a standalone, custom-built system in place?

Response:

Depending upon the system, both are utilized.

172. Would you mind clarifying if there are any existing ERP modules in place, or if you plan to implement new modules as part of this project?

Response:

New modules will not be implemented as part of this project.

173. Please describe the IT Risk Management frameworks (e.g., NIST 800-30, 800-53, etc.) followed by DASNY. (Section 2.1, Phase 1)

Response:

Previous IT audit activities generally reference recognized frameworks and standards, including the NIST Cybersecurity Framework and ISO-based practices, as appropriate, to inform risk identification and prioritization. These frameworks are used as guidance rather than as prescriptive compliance requirements. The Internal Audit function is open to recommendations that align with leading practices and the organization's risk profile.

174. Are information technology processes, policies, and procedures centralized and standardized across systems and locations? (Section 2.1, Phase 2)

Response:

IT policies and procedures are centralized standardized across systems and locations, with limited variations where operational needs require.

175. 15a. If not, please briefly summarize the extent of decentralization/distribution and variation.

Response:

N/A.

176. Where do you host IT systems (in-house data center, cloud services (IAAS/PAAS), or hybrid model)? Are they supported internally or by third parties? (Section 2.1, Phase 2)

Response:

Hybrid, with both internal and third parties support.

177. Please summarize the kinds of IT services and applications that are outsourced or provided by managed service providers (e.g., data center/cloud hosting, help desk, security monitoring). (Section 2.1, Phase 2)

Response:

IT help desk services are managed in-house. However, certain applications and systems are supported by third-party vendors for maintenance, hosting, or specialized support.

178. Do you own or maintain homegrown/proprietary systems? If yes, please specify the purpose of these systems. (Section 2.1, Phase 2)

Response:

Yes, DASNY maintains internally developed systems. Additional details will be provided to the firm selected.

179. On average, how many IT audits do you usually perform annually? (Section 2.1, Phase 2)

Response:

Typically, one to two IT audits are performed annually.

180. Please describe the proportion of fieldwork that needs to be performed remotely, onsite, or both. If onsite, please indicate the location(s) to visit. (Section 2.3)

Response:

All work can be performed remotely.

181. Are there any restrictions on utilizing offshore team members for supporting the engagement? (Section 2.3)

Response:

This type of contract does not allow for the use of offshore team members.