BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services
Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
1	How do you define Audit?	"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes" - Institute of Internal Auditors.
2	Are you looking for your partner to provide a formal SOC2 (either Type 1 or Type 2) certification?	No.
3	Will onsite assessment be preferred or required? If so, for what number of days or percentage of the project?	All services are expected to be performed remotely and onsite, as needed. The number or percentage of onsite days cannot be estimated at this time.
4	Is there an expectation around remote vs. onsite work?	All services are expected to be performed remotely and onsite, as needed.
5	Remote Work Allowance: Will remote work be permitted or is on-site presence mandatory for parts of the assessment?	All services are expected to be performed remotely and onsite, as needed.
6	Are any portions of the audit required to be performed on-site?	All services are expected to be performed remotely and onsite, as needed.
7	How much onsite time do you estimate will be required vs. remote?	The amount of onsite time cannot be estimated at this time.
8	Can all work be performed remotely or is there an expectation of on-site fieldwork? If on-site is required, may travel costs be reimbursed for contractor personnel residing outside of the city?	All services are expected to be performed remotely and onsite, as needed. BERS does not reimburse travel costs.
9	Audit Access & Mode: Will access to systems, personnel, and documentation be entirely remote, or should the vendor plan for onsite visits? If so, how many visits and for which locations?	Systems and documentation access will be available remotely. Onsite work may be needed for certain procedures. BERS does not reimburse travel costs.
10	Can you clarify expectations regarding onsite versus remote activities?	All services are expected to be performed remotely and onsite, as needed.
11	The RFP notes work *"performed remotely and onsite (in-person), as needed."* Can you estimate expected on-site days, office locations besides 55 Water Street, and whether travel costs should be fixed or reimbursable?	Onsite days cannot be estimated in advance. BERS also has offices at 65 Court Street, Brooklyn NY 11201.
12	Will secure virtual desktops or on-prem analysis space be provided if data export is restricted?	Yes.
13	Are there any blackout periods or scheduling restrictions that might impact work?	Scheduling will be coordinated with the vendor during the audit planning stage. If there are blackout periods or scheduling restrictions these will be communicated at that time.
14	Will remote access to systems/logs be provided, and through what means?	Yes, through secure virtual desktop.
15	Will auditors be permitted to take encrypted copies of evidence off-site for analysis, or must all work be conducted within BERS-controlled environments?	All work must be conducted within BERS-controlled environments.

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services
Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
16	Has the New York City Board of Education Retirement System undergone previous information security audits, vulnerability assessments, and penetration testing? What was the expected level of effort or labor hour totals for previous assessments?	Yes, and it was approximately 200 hours.
17	Was a similar audit performed in prior years? If yes, how recently?	Yes, four years ago.
18	When was the last information security audit of this nature performed?	Four years ago.
19	Have there been prior IT security audits or assessments? If so, can previous findings be shared to better scope the engagement?	Yes. Prior findings will be shared with the selected vendor.
20	Have any recent third-party or internal security audits been performed? If so, can those reports be shared to avoid duplicative effort?	Yes. Prior audit report(s) will be shared with the selected vendor.
21	Current Vendor/Supplier: Is BERS currently using any service providers that are assisting the BERS in performing the requested services? If so, who are these providers?	BERS is not currently using internal audit service providers.
22	Effort: Can BERS share estimates or expectations regarding: - Number of systems/applications to be reviewed? - Number of locations or departments to be audited?	Specifics around the number of systems and departments involved should be determined during audit planning. BERS currently has two office locations and two datacenters.
23	How many IT staff members does BERS have? Of these, how many are dedicated to IT security?	BERS currently has nine IT staff members; three are dedicated to IT security,
24	Assessment Framework: Would you want to review controls from PCI-DSS and SOX perspective as well?	No.
25	Previous assessments: Have you done any assessments perviously against any framework?	Yes.
26	Control Implementation Documentation: Is there a documentation on security control implementation available? Would you like this to be updated or created, if needed?	Any available control implementation documents will be shared with the selected vendor.
27	Will the audit workpapers of the most recent Information Security Audit be shared with the selected IT audit firm?	Yes.
28	Access to Existing Documentation: Will previously conducted audits or assessments be shared for review to avoid duplication?	Yes. Prior audit report(s) will be shared with the selected vendor.
29	Other than what is specifically listed in the RFP, are there any other areas of scope, laws, regulations, or frameworks to be covered by the audit?	The frameworks, laws and regulations listed in the RFQ are examples. Applicability and appropriateness will be determined during audit planning.
30	Are there any extra deliverables or audit phases beyond the current scope you'd like included?	No.

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services
Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
31	Is the selected vendor expected to support remediation activities beyond identifying risks and recommendations?	No.
32	Is a follow-up verification of remediation (e.g., 6-month retest) envisioned, and should it be included in the six-month contract or proposed separately?	No. The vendor is not expected to conduct follow-up verification after the audit is concluded.
33	How should findings be prioritized—by inherent risk, residual risk, business impact, or another taxonomy used by BERS?	Findings should be prioritize by residual risk and business impact.
34	Is the New York City Board of Education Retirement System expecting to review the contractor's Audit Work Program and work papers prior to and after the conclusion of fieldwork?	Yes. The Audit Work Program and all other audit workpapers must be made available to BERS.
35	Regarding the Categorization of risks based on impact and likelihood, is the New York City Board of Education Retirement System expecting a risk assessment as a deliverable?	Yes. An audit-specific risk assessment should be documented.
36	Are there specific applications or systems you want prioritized in the audit?	This is to be determined based on the audit-specific risk assessment.
37	Are there particular network segments or infrastructure components that need more thorough examination?	This is to be determined based on the audit-specific risk assessment.
38	Network and Infrastructure: Are there any specific network segments or devices that require special attention during the audit beyond what is mentioned in the RFQ?	This is to be determined based on the audit-specific risk assessment.
39	Are there any recent events or particular concerns that should be emphasized during the audit?	None that we are aware of at this time.
40	Are there particular risk areas or scenarios regarding assets, processes, or architecture that you would like the vendor to concentrate on during the audit?	This is to be determined based on the audit-specific risk assessment.
41	Scope and Objectives: Based on review of the prior 2024 and 2025 Meeting Minutes, it appears there have been breaches that have led to override of controls and misappropriation of assets. Are there any particular areas of concern or focus within your IT infrastructure that you would like us to prioritize beyond what is mentioned in the RFQ?	This is to be determined based on the audit-specific risk assessment.
42	Current Security Posture: Can you share any additional recent incidents or security breaches, above what has been discussed and identified in 2024 and 2025 Meeting Minutes that have occurred, and how they were handled? May you also elaborate on what controls where circumvented to allow the breaches which occurred prior to the RFQ to take place?	BERS is not aware of any additional recent incidents or security breaches. Pertinent information about prior incidents will be shared with the selected vendor, as needed.

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services
Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
43	Governance & Risk Management: Does BERS currently use a GRC tool or framework (e.g., Archer, MetricStream, manual spreadsheets) for tracking controls, risks, and policies? Will access be provided for review?	Information regarding any GRC tools in use will be shared with the selected vendor.
44	Would BERS like optional support to map findings into an enterprise GRC system (e.g., Archer, ControlMap) for continuous tracking?	Information regarding any GRC tools in use will be shared with the selected vendor.
45	Does the audit need to be completed following any particular auditing standard? For example Yellow Book.	Yes. This is audit is to be conducted in accordance with the Global Internal Audit Standards promulgated by the Institute of Internal Auditors.
46	Which NIST (National Institute of Standards and Technology) framework(s) are in scope?	To be determined during audit planning.
47	Which CIS (Center for Internet Security) framework or baselines are in scope (if CIS Critical Security Controls/18, which Implementation Group and are all Safeguards in scope)?	To be determined during audit planning.
48	Which compliance frameworks (such as NIST, CIS, SOC 2, NYC Cyber Command) are most important for BERS to meet?	Of the frameworks listed, NYC Cyber Command, NIST and/or CIS are most important for BERS.
49	Which specific regulations or standards (e.g., NIST 800-53, NIST CSF, SOC 2, NYC Cyber Command baselines) are in-scope for compliance validation?	In scope regulations or standards will be determined during audit planning.
50	Which cybersecurity frameworks and standards does BERS currently adhere to (e.g., NIST, CIS, SOC 2)?	Specifics around cybersecurity frameworks currently adhered to will be discussed during the audit.
51	Beyond the references to NIST, CIS, SOC 2 and NYC Cyber Command, which specific control framework(s) should the final report be explicitly mapped to?	The most appropriate framework will be determined during audit planning. Prior Information Security audit was conducted under the CIS framework.
52	**Item 6.1.1 in the RFQ** requests a compliance assessment against NIST standards. Is this the NIST CSF, NIST SP 800-53, or both?	**RFQ Section 6.1.1 - Governance and Compliance** provides examples of frameworks. The most appropriate framework will be determined during audit planning.
53	Is BERS' IT governance framework aligned with a particular security or control framework, such as the NIST CSF or CIS Controls? If so, which one(s)?	Framework alignment should be assessed during the audit.
54	Is a full NIST 800-53 control-by-control gap analysis required, or are risk-ranked findings sufficient?	The selected framework will be used as criteria where applicable to BERS' IT operations. All controls may not be applicable to BERS. The findings should be risk-ranked.
55	**RFQ Audit Scope Section 6.1.1. Governance and Compliance,** mentions a list of relevant laws, frameworks, and regulations. Will BERS be able provide the selected firm a complete list of relevant laws, frameworks, and regulations?	Information available to BERS will be shared with the selected vendor. The most appropriate framework will be determined during audit planning.

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services
Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
56	Compliance Requirements: Are there any upcoming changes in regulations or new compliance requirements that we should be aware of?	None that we are aware of at this time.
57	Please define Governance and Compliance Service Scope – Is it right to conclude that BERS is requesting the vendor to conduct Risk Assessment Based on the NIST CSF framework, including multiple other frameworks at once? If not, please clarify.	The assessment should not include multiple frameworks at once. The most appropriate framework will be determined during audit planning.
58	What control framework is the New York City Board of Education Retirement System's IT governance based on?	Specifics around the control framework adhered to will be discussed during the audit.
59	Does BERS require mapping of current security controls against one or more of these frameworks?	Yes.
60	Are application mappings and data flows already documented?	This should be assessed during the audit.
61	Does the scope of the audit include compliance with the governance framework, policies, standards, and procedures?	Yes.
62	Approximately how many formal, documented policies, standards, and procedures are in place?	Pertinent information will be shared with the selected vendor.
63	How many policies, standards, and procedures, or other documents are to be included in the audit, and how many pages total?	Pertinent information will be shared with the selected vendor.
64	How many policies, standards, and procedures are in scope for review?	Pertinent information will be shared with the selected vendor.
65	Are there specific IT governance policies or procedures that you want the vendor to review in detail?	In scope policies and procedures will be determined during audit planning.
66	Can you provide information on any recent updates to your IT governance or compliance strategies?	Any recent updates to IT governance or compliance strategies will be shared with the selected vendor.
67	What essential IT processes support your operations, and are there specific ones you want the vendor to assess for security and efficiency?	Refer to Section 6.1 Audit Scope for the areas to covered in the audit. Essential IT processes and the specific ones to be assessed will be determined during the audit.
68	Could you give an overview of your IT architecture and point out any components you suspect may be vulnerable or need special attention?	BERS' IT architecture will be discussed with the selected vendor. Vulnerability will be assessed by the vendor during the audit.
69	Current Architecture: Is current architecture documentation of the system available?	Any available architecture documentation will be shared with the selected vendor.
70	Can BERS provide a high-level network diagram or architectural overview of its IT environment (including cloud-hosted services)?	Pertinent information will be shared with the selected vendor.
71	Application Controls and Access Management: Can you provide details on any recent changes or upgrades to your key systems and applications?	Pertinent information will be shared with the selected vendor.
72	Current Deployment: Is the entire application in Cloud? Hybrid or On Prem?	It is hybrid.

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services
Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
73	Current Support: Is a vendor maintaining your system or Hybrid or all BERC resources (employee and contractors)?	Pertinent information will be shared with the selected vendor.
74	What security controls are currently implemented across your IT environment? Have any been recently updated or identified as inadequate?	Pertinent information will be shared with the selected vendor.
75	Can you provide a detailed list of IT assets included in the audit (hardware, software, cloud platforms), highlighting any critical ones?	This information will be shared with the selected vendor.
76	System and Infrastructure: Can BERS provide an overview or inventory of systems (e.g., cloud environments, legacy systems) to be included in the audit?	This information will be shared with the selected vendor.
77	Please supply an asset inventory (systems, applications, network segments, cloud tenants) with approximate quantities so we may right-size sampling and testing.	This information will be shared with the selected vendor.
78	What are the primary systems, platforms, and applications in use—especially those considered mission-critical?	This information will be shared with the selected vendor.
79	Depth of Testing: What is the approximate size and complexity of the IT environment (e.g., number of IP addresses in scope, applications, databases, user accounts, etc.) to estimate effort?	Pertinent information will be shared with the selected vendor.
80	Application and Infrastructure Details: Can BERS provide a list of critical applications (web, mobile, on-premise, or SaaS) and technology stack used (e.g., Oracle, Microsoft, Java, .NET, etc.)?	This information will be shared with the selected vendor.
81	Please provide the approximate number of servers, workstations, and other devices connected to the internal network?	This information will be shared with the selected vendor.
82	Please provide the number of Active Directory domains.	This information will be shared with the selected vendor.
83	Is BERS' IT function centralized in one location or decentralized in different locations?	This information will be shared with the selected vendor.
84	Can all internal systems be tested/interacted with from one, central location?	This information will be shared with the selected vendor.
85	Which IT processes are outsourced to third-party vendors (if any)?	This information will be shared with the selected vendor.
86	**RFQ Audit Scope Section 6.1.2. Network and Infrastructure Security,** mentions vulnerability assessments and penetration testing. Does BERS expect the selected firm to perform vulnerability assessment and penetration testing? Or rather, review the activity that BERS performs related to vulnerability assessment and penetration testing?	BERS expects the selected firm to perform a vulnerability assessment and review results of any prior penetration tests. The need to conduct penetration testing as part of this audit will be determined during audit planning.

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services
Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
87	Is performance of vulnerability assessments and penetration testing included in the scope, and if so, what is the number and type of systems to be assessed testing, and what kind of testing is to be performed?	BERS expects the selected firm to perform a vulnerability assessment and review results of any prior penetration tests. The need to conduct penetration testing as part of this audit will be determined during audit planning. The number and type of systems to be assessed during the audit will be determined during audit planning.
88	Is the New York City Board of Education Retirement System expecting an internal and external vulnerability assessment and penetration test?	BERS expects the selected firm to perform a vulnerability assessment and review results of any prior penetration tests. The need to conduct penetration testing as part of this audit will be determined during audit planning.
89	For **RFQ Item 6.1.2, Network and Infrastructure Security**, should the vulnerability assessments and penetration tests be performed from both external and internal perspectives?	BERS expects the selected firm to perform a vulnerability assessment and review results of any prior penetration tests. The need to conduct penetration testing as part of this audit will be determined during audit planning.
90	For the vulnerability assessment / penetration testing element, what testing depth is expected (external, internal, wireless, web app, social-engineering, red-team)? Are any methods or targets explicitly out of scope?	BERS expects the selected firm to perform a vulnerability assessment and review results of any prior penetration tests. The need to conduct penetration testing as part of this audit will be determined during audit planning.
91	Will the selected vendor be granted system access (e.g., read-only or full administrative) for vulnerability assessments and penetration testing?	Yes. The level of systems access will be determined during the audit.
92	What security tooling (SIEM, EDR, IDS/IPS, DLP, CASB, cloud CSPM, etc.) is currently deployed, and what level of read-only or log-export access will the auditor receive?	Pertinent information will be shared with the selected vendor.
93	Is web application penetration testing in scope? If so, of how many URLs? Will credentials be provided?	This will be determined during audit planning.
94	Is a wireless network penetration test in scope? If so, is the wireless network controller based? If not, how many locations and approximately how many access points are in scope?	This will be determined during audit planning.
95	Is New York City Board of Education Retirement System looking for a M365 and/or AWS vulnerability assessment?	The specifics of any vulnerability testing will be determined during audit planning.
96	How many Azure/AWS/Google/M365 tenants does New York City Board of Education Retirement System have?	Pertinent information will be shared with the selected vendor.
97	Please describe the use of Google / Azure / M365 / AWS, including licensing / subscription level.	Pertinent information will be shared with the selected vendor.
98	Please describe the data and other infrastructure and systems you presently have in Google / Azure / M365 / AWS.	Pertinent information will be shared with the selected vendor.

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services

Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
99	Can an approximate number of applications, servers, and IP address that would be in scope for vulnerability scanning and penetration be provided?	Pertinent information will be shared with the selected vendor.
100	How many applications/systems would be in scope for this audit?	Five or more.
101	Are these applications/systems developed and maintained internally or off-the-shelf software?	The applications in use by BERS are not developed and maintained internally.
102	Are these applications/systems hosted internally or at third-party datacenters?	The majority of the applications in use by BERS are hosted by third party vendors.
103	How many active public IP addresses are in use (have a service exposed to the Internet)?	Pertinent information will be shared with the selected vendor.
104	Approximately how many live external IP addresses are in scope?	Pertinent information will be shared with the selected vendor.
105	Approximately how many internal IP addresses are in scope? Can they all be reached from a central location?	Pertinent information will be shared with the selected vendor.
106	Are we reviewing the results of the penetration testing and vulnerability scanning BERS is already performing, or are they expecting us to perform that testing for them?	BERS expects the selected firm to perform a vulnerability assessment and review results of any prior penetration tests. The need to conduct penetration testing as part of this audit will be determined during audit planning. Existing results of prior vulnerability assessments should also be reviewed.
107	Do you have preferred tools or approaches for conducting vulnerability assessments and penetration tests?	No.
108	Given the scope of your external network vulnerability assessments, can you please specify the number of IP addresses that need to be evaluated?	Pertinent information will be shared with the selected vendor.
109	For Internal Network Vulnerability Assessment and penetration testing, please share the following: - Size of Internal Network: (IPs)? - No of devices (Laptop/Desktop/Printers etc.) - No of Network Devices - No of AD (Active Directory) - Active Directory Scanning being part of the Scope. - Location Specifications and Network Connectivity Details. - If Cloud Environment part of the scan.	Pertinent information will be shared with the selected vendor.
110	Is a retest of found vulnerabilities required?	This will be determined during the course of the audit.
111	Will penetration testing include external, internal, or both? What limitations or constraints (e.g., IP ranges, timing) should we be aware of?	This will be determined during audit planning. Pertinent information will be shared with the selected vendor.
112	What is the total number of assets that need to be penetration tested?	Pertinent information will be shared with the selected vendor.

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services
Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
113	Please provide an overview of the organization's current firewall infrastructure, including the count &, if possible, type of firewalls (e.g.; – NextGen with Make and Model) deployed. Please specify if any Disaster Recovery Firewall is in place.	Pertinent information will be shared with the selected vendor.
114	What brand of firewalls, VPNs, IPS, IDS are in use and how many appliances are in scope for the review?	Pertinent information will be shared with the selected vendor.
115	Is a comprehensive review of all firewall configurations necessary, or can a representative sample be selected? If sampling is acceptable, please specify the desired sample size or provide guidance on selecting appropriate firewalls for review.	This will be determined during the course of the audit.
116	Please confirm whether you require only a firewall configuration review or if a log review is also necessary. If a log review is required, please specify the estimated volume of logs (in GB) that need to be analyzed.	This will be determined during the course of the audit.
117	Please specify the primary areas of focus for the firewall review. Choose from architecture, security, performance, compliance, or other. If you select 'other,' please provide more details.	Specifics of any firewall reviews will be determined based on audit-specific risk assessment and during planning.
118	What is the brand of firewall you currently utilize?	Pertinent information will be shared with the selected vendor.
119	How many firewalls are being evaluated?	Pertinent information will be shared with the selected vendor.
120	How many firewalls are in scope for configuration reviews? Are any of these paired, or in HA mode?	Pertinent information will be shared with the selected vendor.
121	Approximately how many rules per firewall enforcement point?	Pertinent information will be shared with the selected vendor.
122	How many of what type of firewall and other network security devices configurations are to be reviewed?	Pertinent information will be shared with the selected vendor.
123	What is the approximate size and complexity of BERS' network (e.g., number of sites, firewalls, VPNs, servers)?	Pertinent information will be shared with the selected vendor.
124	What is the current condition of your firewall setups, VPNs, and IDS/IPS solutions? Are there any known issues or priorities?	Pertinent information will be shared with the selected vendor.
125	How many servers virtual and on premise do you have?	Pertinent information will be shared with the selected vendor.
126	How many applications are in scope for **RFQ Section 6.1.3 - Application Controls and Access Management?** Are these exclusively on-premises systems? Are any hosted in the cloud?	Five or more cloud based and on-premises.
127	For applications that are cloud-based, do we have the authority to audit them?	Yes.

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services
Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
128	Is authentication to all of these systems controlled via Active Directory?	Pertinent information will be shared with the selected vendor.
129	Is this managing audit for all mobile devices? How many and types by operating system?	During audit planning, the determination will be made as to whether mobile devices are included in the audit.
130	Please share VPN setup details: tool in place, number of users, etc.	Pertinent information will be shared with the selected vendor.
131	Can you list the advanced functions per FW enforcement point (IPS, Sandboxing, VPN, DNS)?	Pertinent information will be shared with the selected vendor.
132	Please explain the type and count of Key Systems and application: Evaluate the internal controls over key systems and applications, including access controls, input/output data processing, and system integrations.	Pertinent information will be shared with the selected vendor.
133	Application and Infrastructure Details: Are any cloud environments (e.g., AWS, Azure, GCP) in scope? If yes, please clarify if tenants/accounts across multiple cloud services will be audited.	Yes. Specifics around tenant account audit will be determined during the course of the audit.
134	Are cloud services (e.g., SaaS, IaaS) in-scope, and if so, which providers?	Cloud services are in scope. Information regarding providers will be shared with the selected vendor.
135	Are cloud-based systems (e.g., AWS, Entra ID, GWS) in scope for the audit, and if so, what percentage of BERS infrastructure is cloud-hosted?	Yes. Pertinent information will be shared with the selected vendor.
136	What cloud providers do you use, i.e.; Azure, Google, AWS?	Pertinent information regarding providers will be shared with the selected vendor.
137	What cloud service providers are currently used by the New York City Board of Education Retirement System?	Pertinent information regarding providers will be shared with the selected vendor.
138	Are there any cloud providers or related contracts you want us to assess?	This will be determined during the course of the audit.
139	Please define the scope and type of services to be evaluated which are provided by cloud service provider?	Pertinent information will be shared with the selected vendor.
140	How many cloud service provider agreements/security controls are to be assessed, and against which standard? Is this is review of available materials or do we need to request documentation or make observations and/or audit these vendors?	Five or more. Standard that is most appropriate to BERS will be determined during audit planning. The audit will cover applications in use, not the vendors.
141	How many cloud service provider agreements should we expect to review?	Five or more.
142	For the audit generally, how many systems, networks, locations, cloud tenants, and/or other separate environments are in scope?	Five or more.
143	Are there any systems hosted by a 3rd party that you are going to get permission to include in the scope of the external testing? Describe these systems.	Yes. Pertinent information regarding the systems used will be shared with the selected vendor.

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services

Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
144	Third-Party Risk Assessment: How many critical third-party vendors or cloud service providers (CSPs) are expected to be part of the audit's third-party risk management review?	Pertinent information will be shared with the selected vendor.
145	Third-Party Risk Management: Are there any specific third-party vendors or cloud service providers that you are particularly concerned about?	Pertinent information will be shared with the selected vendor.
146	Third-Party Risk Assessment: Will contract reviews or direct interviews with vendor stakeholders be required?	This will be determined during the course of the audit.
147	Could you explain your current Identity and Access Management processes, including any challenges with access controls?	Pertinent information will be shared with the selected vendor.
148	How many privileged user accounts exist, and what is the status of your multi-factor authentication implementation?	Pertinent information will be shared with the selected vendor.
149	Does BERS have a formal data classification policy?	Pertinent information will be shared with the selected vendor.
150	Has sensitive data, such as PII, been inventoried across the IT environment?	Pertinent information will be shared with the selected vendor.
151	Has BERS classified systems based on the sensitivity of the data that they contain?	Pertinent information will be shared with the selected vendor.
152	What types of sensitive data (e.g., personal identifiable information, financial data) require safeguarding?	Pertinent information will be shared with the selected vendor.
153	Are there particular data privacy laws or regulatory requirements that must be addressed in this audit?	Applicable data privacy laws or regulatory requirements in scope will be determined during audit planning.
154	What type of controls do you have for "Assessment of controls for personally identifiable information ("PII") and financial data" and are you looking for controls recommendations?	Controls in place will be discussed with the selected vendor. Actionable control recommendations are expected.
155	Data Protection and Privacy: How do you handle data retention and disposal, especially for personally identifiable information (PII) and financial data?	Pertinent information will be shared with the selected vendor.
156	Is the incident response plan formal and documented? When was it last tested?	Pertinent information will be shared with the selected vendor.
157	Are the business continuity and disaster recovery plans formal and documented? When were they last tested?	Pertinent information will be shared with the selected vendor.
158	Can BERS please provide copies of current incident response and disaster recovery plans in advance for review?	Documents will be shared with the selected vendor.
159	Incident Management: Can you share any recent updates or changes to your incident response plans and disaster recovery protocols?	Pertinent information will be shared with the selected vendor.

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services
Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
160	Have the current incident response and disaster recovery plans been tested recently (e.g., tabletop or live exercises), and will those test results be made available?	Pertinent information will be shared with the selected vendor.
161	Has your organization recently reviewed or tested its incident response and disaster recovery plans?	Pertinent information will be shared with the selected vendor.
162	Please define scope for evaluation of Disaster Recovery and BCP? Also, is the vendor expected to only focus on complete less and validation of the plans by interviewing the SMEs about critical business applications?	BERS expects the selected vendor to review existing DR and BCP documents and provide actionable recommendations.
163	Would BERS like the vendor to evaluate the effectiveness of recent incident responses or business continuity efforts?	Yes.
164	How many applications are in-scope for access control reviews, and are any cloud-hosted?	Five or more.
165	What IAM tools or platforms are currently used (e.g., Okta, Azure AD, etc.)?	Pertinent information will be shared with the selected vendor.
166	Which identity platforms (e.g., Microsoft Entra ID, on-prem AD, Okta, PAM tooling) are in scope for the IAM and privileged-access reviews?	Pertinent information will be shared with the selected vendor.
167	What types of data storage systems are in use (e.g., on-premises servers, cloud storage, databases)?	Cloud and on-premises.
168	What is the volume of data being stored, and how is it expected to grow over the next (Number) years?	Pertinent information will be shared with the selected vendor.
169	What specific data requires encryption (e.g., data at rest, data in transit, both)?	Pertinent information will be shared with the selected vendor.
170	Which encryption methods are currently in use (e.g., AES-256, RSA, TLS)?	Pertinent information will be shared with the selected vendor.
171	Where is the encryption performed (e.g., application-level, database-level, full-disk encryption)?	Pertinent information will be shared with the selected vendor.
172	What data protection solutions are currently deployed (e.g., DLP, encryption technologies)?	Pertinent information will be shared with the selected vendor.
173	Are there additional NYC or BERS encryption, retention, or destruction requirements beyond those already listed in **Appendix A - BERS Terms and Conditions?**	See the following: https://www.nyc.gov/site/records/about/policies.page Note that BERS keeps member/retiree records indefinitely.
174	Will the audit include data loss prevention or cloud storage solutions (e.g., OneDrive, SharePoint, AWS S3)?	Yes.
175	Do you have processes in place for monitoring and evaluating third-party vendor security controls?	Yes.
176	Approximately how many vendor relationships are in place for IT services?	Five or more.

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services
Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
177	How many third-party vendors does BERS work with, and what are the primary risk considerations related to them?	Five or more. Third-party risk management processes should be assessed during the audit.
178	How many third-party vendors with network/system access will be reviewed?	Five or more.
179	Will NYC BERS consider the inclusion of the vendor's applicable service schedules, which may include third party end user license agreements, that may be incorporated into the final contract between the parties?	We can review on a case by case basis.
180	Is it expected from the selected IT audit firm to develop their own audit work program? Or is BERS expecting the selected IT audit firm to use a publicly available IT control framework?	The selected firm will develop an audit work program. Publicly available IT control frameworks such as NIST, CIS, COBIT, etc. may be used.
181	For which of the scope areas does BERS rely on a NYC-shared IT service?	This information will be shared with the selected vendor.
182	Would BERS accept the use of offshore resources by the selected IT audit firm (mainly for testing of controls and workpaper documentation)?	No. The use of offshore resources is not acceptable.
183	Exploring Hybrid Options: Is BERS open to exploring non-USA/offshore based hybrid options to provide the requested services and solutions? Our clients typically want to leverage this option to get access to our global pool of cybersecurity professionals in a cost-efficient manner.	No. The use of offshore resources is not acceptable.
184	Can BERS confirm whether Indian firms are eligible to participate in the current ("this") RFQ process.	No. The use of offshore resources is not acceptable.
185	We are a Cyber Security Consultancy based in the United Kingdom with a global customer base. Would we be able to be considered for the services that are applicable?	No. The use of offshore resources is not acceptable.
186	Additionally, we would appreciate it if you could kindly advise us on any key compliance points or specific aspects we should take care of while preparing our submission, to ensure our proposal aligns with BERS' expectations and requirements.	Proposers are advise to carefully review the entire RFQ solicitation, including all requirements, scope, and award criteria and to structure their proposals addressing all areas.
187	Under **RFP Section 13 - Basis of Award**, the last two paragraphs seem to conflict. The first indicates negotiations will be conducted, the second indicates vendors must be willing to comply with **Appendix A – BERS Terms and Conditions**, without negotiation. If BERS is willing to negotiate, do you want vendors to identify the points for negotiation/exceptions in the proposal?	We are willing to negotiate to a point. Some items may not be negotiatiable. Please identify points for negotiation in your proposal.

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services
Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
188	Are exceptions allowed?	Regarding **Appendix A - BERS Terms and Conditions,** we are willing to negotiate to a point. Some items may not be negotiatiable. Please identify points for negotiation in your proposal.
189	Is the response binding?	Yes.
190	Will a pricing template be forthcoming or are there specific formatting requirements?	There is no pricing template or specific formatting requirements. Per **RFQ Section 7 - Pricing Proposal (Budget),** *"Respondents must submit a Pricing Proposal (Budget) that provides detailed line-item pricing for the proposed deliverables/services."* Proposers are strongly advised to carefully review **RFQ Section 7 - Pricing Proposal (Budget)** in its entirety.
191	Does BERS prefer firm-fixed pricing by deliverable, blended hourly rates, or a not-to-exceed model with capped hours?	Vendors should propose the most effective pricing model based on the services they intent to provide based on the RFQ requirements and scope of services. Vendors are advised that regardless of the proposed pricing model (whether unit prices, hourly rates, fee for service, flat rate, licensing fee, or any combination of these), per **RFQ Section 7.4,** *"Unit prices/fees are maximum, not-to-exceed amounts that will be incorporated into the contract. Unit prices/fees proposed (or any component thereof) are not subject to upward adjustment."*
192	Under Appendix C – Approach and Methodology, NYC BERS asks for a detailed program plan. Is this meant to be a timeline plan for implementation or just an outlined plan of how the solution will be implemented?	Please note, under **RFQ 2025-001, Appendix C is Basis of Award Criteria.** Under **Award Criteria Section 13.2 - Approach and Methodology,** proposers must provide detailed description on how they indend to tackle/perform/execute/implement the required services, including, but not limited to, methods, technique, processes, resources, plans, procedures, timeline, etc.
193	How will cost be weighted against technical quality in the "Best Value" assessment?	Please refer to **RFQ Section 13 - Basis of Award, Subsection 13.4 - Cost Effectiveness.**
194	Will BERS consider extending the submission due date?	Yes, please refer to **RFQ Addendum No. 2,** where the new RFQ Submission Deadline is **no later than 4:00 P.M EST on June 20, 2025.** Proposers are advised that **late submissions will not be accepted.**
195	Beyond CISA/CISM/CRISC, will credentials such as CISSP, CIPP/US, or ISO 27001 Lead Auditor satisfy the certification requirement?	The certifications noted do not satisfy the certification requirements listed in RFQ Section 5.3.
196	Could BERS please confirm whether vendors are required to provide their responses directly in the spaces provided within the RFQ document under 'APPENDIX B: MINIMUM QUALIFICATIONS REQUIREMENTS' (page 29) and 'APPENDIX C: BASIS FOR AWARD CRITERIA' (page 35), or if it is acceptable for vendors to submit their responses to these sections using their own format (e.g., Word or PDF)?	Proposers may submit their responses to **Appendix B – Minimum Qualifications Requirements** and **Appendix C – Basis of Award Criteria** using their own format (e.g.: Word or PDF), as long as all required information and documents are submitted, they are clearly labeled, and the logical sequence of each appendix section is maintained, i.e., Appendix B, Section 5.1, 5.2, etc. and Appendix C, Section 13.1, 13.2, and so on. Proposers are also reminded they must submit a Pricing Proposal (Budget) per **RFQ Section 7 - Pricing Proposal (Budget).**

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services
Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
197	Please provide clarification regarding pages 29–32 of the RFQ, specifically **Appendix B: Minimum Qualifications Requirements.** Are we required to use the exact forms provided in the RFQ for submission, or may we present the required information within our overall proposal format, as long as all requested details are clearly addressed?	Please refer to the response to question 196, above.
198	Can vendors respond to requirements in Appendices B and C using their own proposal templates?	Yes, please refer to the response to question 196, above.
199	Could you please confirm whether there is a character or page limit for the response fields provided in the text boxes within the solicitation documents?	There is none. Proposers may use as much space as necessary when crafting their proposal response, but please be concise.
200	Are vendors permitted to increase the size of the text boxes to accommodate complete responses?	Yes. Also, please refer to the response to question 199 above.
201	Could the BERS please confirm whether this is a new initiative or an existing engagement?	This would be a new engagement.
202	Could the BERS provide an estimated budget or a Not-to-Exceed (NTE) amount for this contract?	No. BERS cannot provide an estimated budget or not-to-exceed amount.
203	Do you have a set budget for this work or some estimated fee range?	Yes.
204	Can the maximum budget value be provided?	No. BERS cannot provide a maximum budget value.
205	Budget: Can BERS provide any information on the budget required to support these services? (e.g., budget details).	No. BERS cannot provide budget information.
206	Budget and Pricing: Can you provide more details on any budget constraints or preferences for the pricing model?	No additional information can be provided.
207	Should optional post-remediation validation services be priced now or proposed as future time-and-materials?	Vendors may not propose optional post-remediation validation services.
208	Please provide contract award amounts for the previous Information Security Audits, Vulnerability Scanning, and Penetration Testing.	Prior related engagements addressed different components than those specified in this RFQ. As such, details regarding prior contract award amounts are deemed not relevant.
209	Could the BERS please provide the anticipated project timeline, including key milestones and the overall expected duration of the engagement?	Please refer to RFQ Section 6.1: Audit Scope, Section 6.2: Audit Phases and Deliverables, and Section 10: Contract Term.
210	Timeline and Audit Planning: Will BERS mandate fixed milestones for each phase (e.g., Planning in August, Fieldwork in September–October, Reporting in November), or can the schedule be jointly finalized during project kickoff?	The schedule can be jointly finalized during project kickoff.

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services
Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
211	With contract start *"on or about August 2025"* and completion by December 2025, do you have preferred milestone dates for Planning, Fieldwork, and Reporting, or blackout periods (e.g., fiscal close) we should avoid?	The schedule can be jointly finalized during project kickoff.
212	Timeline and Milestones: Are there any critical milestones or deadlines we need to be aware of beyond what is mentioned in the RFQ?	None at this time.
213	Is there is a specific date or timeframe in which the audit needs to be completed by?	No. The schedule can be jointly finalized during project kickoff.
214	**RFQ Section 10 "Contract Term"** states that the term of this contract (if awarded) will be six (6) months and a possible one (1) month extension. However, this section also indicates the anticipated period of performance is "begin on or about August 2025 and are expected to be completed no later than December 2025," which is only five (5) months. Please confirm the anticipated performance period.	BERS expects the project to be completed within a three or four-month timeframe. However, if there are unanticipated delays, the project timeline may be extended.
215	Could the BERS please clarify whether it intends to award this RFQ to a single vendor or multiple vendors? If multiple awards are anticipated, could the BERS specify the expected number of vendors to be selected?	BERS intends to select a single vendor.
216	Can the vendor scoring – selection criteria be provided?	Yes, please refer to **RFQ Section 13 - Basis of Award.**
217	**RFQ Section 6.2.3 - Reporting Phase (p4):** Please confirm that the audit report will only be distributed internally to intended users (internally to BERS and BERS' intended external stakeholders); however, the audit report will not be made available to the public.	The audit report will be distributed internally within BERS, including its Board of Trustees. However, this document or portions thereof may be subject to FOIL.
218	**RFQ Section 6.2.3 - Reporting Phase (p4):** Given the sensitivity of information security audit findings and the potential for such details to be exploited by adversaries, please confirm that the presentation of key findings to BERS' Audit Committee and Senior Management will remain confidential and will not be made publicly available?	An assessment of information that can be shared publicly will be made prior to dissemination of information.
219	**Per Section 9 "Subcontractors"** of the RFQ, please confirm that the use of subcontractors is allowed.	Confirmed.
220	Do you have an example of a reference letter that will fit your needs?	We have no preference as to the format of the reference letters, as long as they contain all the equested information per **RFQ Section 5.5 - Minimum Qualification Requirements.**
221	For the reference letters requirement, do you want us to attach the letters to our proposal or have the clients forward them to you separately?	The letters must be included with the vendor's proposal.

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services
Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
222	Can you prioritize which references would be most beneficial to you in relation to the scope?	Proposers must provide at least three (3) letters of reference from previous engagements within the last five (5) years where similar services were rendered.
223	Is BERS open to negotiating limitation-of-liability, confidentiality, and indemnification language in **Appendix A - BERS Terms and Conditions,** or must those terms be accepted as-is?	To a point. It will depend on proposed changes. Please submit along with your proposal.
224	Do the Whistle-blower and NYC Paid Safe-and-Sick-Leave provisions impose any additional obligations on out-of-state personnel?	No.
225	Communication and Collaboration: Who will be the primary point of contact for this project, and how do you prefer to communicate and collaborate throughout the audit process?	The Director of Internal audit will be the primary point of contact. Communications via email and videoconferencing is preferred.
226	Who will be the main points of contact during the engagement (e.g., IT, legal, compliance, executive sponsors)?	The Director of Internal audit will be the primary point of contact.
227	Will a single BERS liaison coordinate interview scheduling and document collection, and what level of executive access (CISO, CIO, Audit Committee) can we expect during fieldwork?	Yes. The Director of Internal audit will be the primary point of contact. There will be no undue restrictions on the accessibility of members of the BERS IT team.
228	What level of detail is expected in the audit report (e.g., executive-level summaries, technical appendices)?	A comprehensive audit report, including an executive summary, appendices, etc. is expected.
229	Is there a preferred report template or required format for the draft and final audit reports?	BERS internal audit has an audit report template that can be shared with the vendors.
230	Will the final presentation of findings be delivered to both technical staff and the Audit Committee?	Yes.
231	How many formal presentations are expected (e.g., interim read-out, Audit Committee, Board) and what length/depth do you anticipate for each?	One formal presentation to the BERS Audit Committee is expected. Audit Committee meetings are usually scheduled for approximately 1 hour and 30 minutes. The length of the presentation could be up to 30 minutes.
232	What background-check or NYC fingerprinting process is required for audit personnel, and how long does that clearance typically take?	Per **RFQ Section 15 - PASSPort Disclosure Filing,** *"All organizations intending to do business with the City of New York should complete an online disclosure process to be considered for a contract."* The selected vendor, including any subcontractors, will be required to file PASSPort disclosure forms in order for BERS to complete its internal background process prior to contract approval. Timeline for the background process will depend if the selected vendor (and their subcontractor/s) is currently registered in PASSPort and their filing is up-to-date. There is no fingerprinting requirement for this engagement.

BERS Board of Education Retirement System of the City of New York

RFQ 2025-001 Information Security Audit Services
Questions and Answers (Q&A) Document - Date: 05/30/2025

#	Questions	Responses
233	What is the approval workflow for any subcontractor resources we may propose under Section 9?	Per **RFQ Section 9 - Subcontractors,** vendors must include in their proposals complete details and information of any and all subcontractors they intend to use in the execution of the proposed services, including name, contract information, and description of the portion of the work to be performed by any subcontractor(s). Subcontractors will undergo the same background process as the selected vendor.

[END OF DOCUMENT]