|  |  |  |
| --- | --- | --- |
| ETF_logo_large | **STATE OF WISCONSIN**  **Department of Employee Trust Funds**  **A. John Voelker**  SECRETARY | 4822 Madison Yards Way  Madison, WI 53705-9100  P. O. Box 7931  Madison, WI 53707-7931  http://etf.wi.gov |

Date: July 25, 2024

To: All Potential Proposers to RFPs ETD0060

RE: Addendum No. 2 to Request for Proposals (RFPs) ETD0060

IT Audits and Consulting

This Addendum is available on ETF’s web site at <https://etf.wi.gov/node/38681>

**Acknowledgement of receipt:**

**Proposers must acknowledge receipt of this Addendum No. 2 by providing the required information in the table below and including this Page 1 with their Proposal cover letter.**

|  |  |
| --- | --- |
| Company Name: |  |
| Authorized Person (Printed/Typed Name and Title): |  |
| Date: |  |

The following vendor questions and Department answers are hereby added to the RFP:

**RFP ETD0060 for IT Audits and Consulting**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q# | RFP / Appendix # and Section # | Page | | Vendor Question/Rationale | Department Answer |
| Q1 | General Question | N/A | | Please describe your audit methodology at a high level that we would be expected to follow. | The Department expects the audit is risk-based. At a high-level, the audit should follow the process of initial planning, risk identification and assessment, detailed process understanding to refine risk assessment and evaluate controls in place, performing appropriate testing, and reporting. |
| Q2 | General Question | N/A | | Please describe how you scope and estimate hours for your audits? Is there a methodology or framework you follow to estimate hours based on scope or level of testing. Related to this, do you an estimated range of hours you expect for the various audits listed in the RFP? | Hours should be based on scope and level of testing to achieve assurance/support conclusion. It should correspond to the audit methodology based on the general understanding / reasonable assumptions of the IT and security environment. Estimated hours cannot be in a range for a particular engagement. |
| Q3 | General Question | N/A | | For any of the audits planned and included in this RFP, have these areas been audited before?  If so, will open audit issue follow up be included as part of this effort? Also, is it within the scope of responsibility for the new service provider to test/validate closure of past IT audit issues? | Follow-up audits are not in scope. |
| Q4 | 5.1.A.i | 19 | | Can you provide a listing of the applications/systems that will be in scope? | The Department has various COTS, SaaS, and custom developed applications (approx. 20) that are a part of the business function. |
| Q5 | 5.1.A.i | 19 | | Would you like privileged/elevated access included within scope? If so, to what extent? | Yes. |
| Q6 | 5.1.A.i | 19 | | Is there a centralized process for managing user account administration or does each (application, infrastructure, networking) team manage access separately? | Application access is a centralized process managed by the ETF IAM team. Access to infrastructure is managed separately depending on the system. |
| Q7 | 5.1.A.i | 19 | | What tools are utilized to manage the user account administration process? | Depends on the system. The Department uses standard tools from Microsoft and a custom developed tool for the Department’s custom developed applications. |
| Q8 | 5.1.A.i | 19 | | Can you provide a listing of the controls in scope for testing? | CIS – CIS 8.x controls for Account Mgmt, Access Control, Network Monitoring, Incident Response |
| Q9 | 5.1.A.ii | 19 | | For external penetration testing, how many external IP addresses will be included in the testing? | Approx. 40 externally facing IP’s |
| Q10 | 5.1.A.ii | 19 | | For internal vulnerability scanning, how many internally network connected devices will be included in the testing? | Total of 120 servers and at this time 40 customer endpoints (10% of the customers). |
| Q11 | 5.1.A.ii | 19 | | For the physical social engineering, how many locations are in scope? | One. |
| Q12 | 5.1.A.ii | 19 | | Is internal penetration testing in-scope? If so, what are the main objectives for the internal penetration testing activities? | Yes. Objectives outlined in the RFP. |
| Q13 | 5.1.A.ii | 19 | | Is email phishing in-scope? If so, how many employees and how many different phishing campaigns will be included in the testing? | Yes, 400 employees for a generic campaign and 30 or so for a targeted crafted campaign. |
| Q14 | 5.1.A.ii | 19 | | Is wireless network security testing in-scope? If so, how many locations and SSIDs will be included in the testing? | Yes, 1. |
| Q15 | 5.1.A.ii | 19 | | Is web application security testing in-scope? If so, how many web applications and interactive web pages will be included in the testing? | 18 web apps to test. |
| Q16 | 5.1.A.ii | 19 | | Are there any additional penetration testing activities not mentioned above that you would like included in the proposal? If so, please describe the scope of the testing. | Pen test of an endpoint device (laptop) in a typical work-from-home scenario. |
| Q17 | 5.1.A.iii | 19 | | Can you share the methodology and results of the previous risk assessment? (We want to be sensitive to changing internalthe methodology as this may significantly alter the results of the assessment). | Please see Appendix B of the [audit plan](https://etf.wi.gov/boards/audit/2023/06/22/aud7a/download?inline=) |
| Q18 | 5.1.A.iii | 19 | | How many and what level of stakeholders were interviewed/surveyed during the previous assessment? Would you change the number of level of stakeholders this time? | Between 10 to 20, including subject matter experts, section supervisors, bureau directors, and senior management. No. |
| Q19 | 5.1.A.iii | 19 | | How involved was the Audit Committee in the risk assessment process? Were they interviewed? | Input and feedback from the Committee Chair were requested and considered. |
| Q20 | 5.1.B.i | 19 | | Can you share a diagram or technical specifications of the data integrations that exist? | Not at this point, but it can be shared at the point of the engagement or negotiations. |
| Q21 | 5.1.B.i | 19 | | Are all data integrations in scope or will there be a risk assessment to drive priority on which integrations should be tested? | The Department is open to a risk-based approach, but it can be shared at the point of the engagement or negotiations. |
| Q22 | 5.1.B.i | 19 | | Are tools currently being utilized to monitor the success/failure of data movement? If so, please provide details on the tooling and extent of its use. | All APIs are managed through the AnyPoint platform, which includes real time dashboard monitoring as well as alerts staff when APIs are out of bounds on a wide array of metrics, including response time, request counts, error codes, and memory utilization. ETF’s SFTP system also moves data and will alert when there are failures. |
| Q23 | 5.1.B.i | 19 | | Who is ultimately responsible for monitoring the completeness and accuracy of data movement (business or IT)? | Ultimate responsibility falls on IT. |
| Q24 | 5.1.B.i | 19 | | Can you provide a listing of the controls that are currently in place to validate completeness and accuracy of data movement? | Not at this point, but it can be shared at the point of the engagement or negotiations. |
| Q25 | 5.1.B.ii | 19 | | Is the focus of this audit specific to applications or does it include any infrastructure as a code that might be utilized? | The audit is focused on the applications. |
| Q26 | 5.1.B.ii | 19 | | Can you provide a listing of the applications that will be in scope? Additionally, can you provide details on the systems use/purpose, programming language, location (on-premise, hosted cloud, vender cloud, etc.)? | Not at this point, but it can be shared at the point of the engagement or negotiations. |
| Q27 | 5.1.B.ii | 19 | | Is there a centralized process for managing all changes or does each application team manage change separately? | Yes, there is a centralized process. |
| Q28 | 5.1.B.ii | 19 | | What tools are utilized to manage the change process? | Tools used are Ivanti, JIRA, and GitHub |
| Q29 | 5.1.B.ii | 19 | | Can you provide a listing of the controls in scope for testing? | CIS-CSC v8.1 Control 16 Application Software Security |
| Q30 | 5.1.B.iii | 19 | | How is the IT Contingency Plan structured? | It’s structured by business process. |
| Q31 | 5.1.B.iii | 19 | | Please describe the scope of the insurance administration system that was recently implemented. | The Insurance Administration System will be implemented in July 2025 to administer and support multiple insurance benefit programs. |
| Q32 | 5.1.B.iii | 19 | | Will the audit team have to work with any 3rd parties as part of the audit? | No. |
| Q33 | N/A | N/A | | Is this the first time that you will contract a vendor for the services in question? If not, then would a copy of the final contract and amount of the previous successful vendor be available? | See the prior RFP and contract at <https://etf.wi.gov/node/38631> |
| Q34 | N/A | N/A | | Is there a not-to-exceed budget for this project that you can share? | The Department chooses not to answer this question. |
| Q35 | 5.1.A and B | 19 | | For the scope services required for FY 25 and 26, can you confirm that the technical environment in scope and your responses to the questions related to the project have not changed at all since the 2019 RFP addendum #2 that is referenced in the latest RFP? Alternatively, please detail all the changes so that we can scope and price accurately. | Pease see responses to other relevant questions. |
| Q36 | 5.1.A | 19 | | For the external network penetration test, how many live external IPs are in scope? | Approx. 40 |
| Q37 | 5.1.A | 19 | | For the internal network penetration test, how many live internal IPs are in scope? | Approx. 120. |
| Q38 | 5.1.A | 19 | | How many web applications are in scope for web application penetration testing? Will test accounts be provided? | See response to Q15. |
| Q39 | 5.1.A and B | 19 | | Please provide a high-level description of your IT infrastructure and operations in order to get an idea of the level of complexity, sophistication, and nature of implementation. | This can be provided during contract negotiations. |
| Q40 | 5.1.A | 19 | | How many scenarios would you like performed for physical social engineering? Is phishing to be performed as well? How many users in total will be targeted across all scenarios? | Two scenarios, one general and one for a targeted audience.  Yes, phishing is included. 400 employees for a generic campaign and 30 or so for a targeted crafted campaign. |
| Q41 | 5.1-A-i | 19 | | How many systems and/or applications would a typical new hire be granted access to? | Depends on the business area and role. it could vary from a couple to approx. 10. |
| Q42 | 5.1-A-ii | 19 | | How many internal IP addresses, external IP addresses, and applications are in scope for the penetration test? | See responses to Q9, Q36 and Q37. |
| Q43 | 5.1-B-i | 19 | | How many integration points and data flows are in scope? | 5-10 depending on how they are counted. The Department has a mixture of API and file exchanges. There are about 11 data flows. A detailed document can be provided closer to the engagement. |
| Q44 | 5.2-C | 20 | | Should a separate audit report be developed for each audit type or a single audit report for each fiscal year? | A separate audit report should be developed for each project. |
| Q45 |  |  | | How many physical locations does your organization have? | One. |
| Q46 |  |  | | How many users does your organization have? | The Department has about 400 employees. |
| Q47 |  |  | | How many team members does your organization have? | See response to Q46. |
| Q48 |  |  | | How many IT/security team members does your organization have? | Approximately 60 IT staff and 11 security staff. |
| Q49 |  |  | | How many servers does your organization have? | Approximately 130. |
| Q50 |  |  | | How many endpoints do you have? | See response to Q10. |
| Q51 |  |  | | What are the compliance requirements? | State and federal regulations, including HIPAA. |
| Q52 |  |  | | What is the current state of your security policies, procedures, and documentation? | The Department has a comprehensive list that is updated as necessary and reviewed at least every 3 years. |
| Q53 |  |  | | How many external IP addresses are assigned to WI ETF? | ~40. |
| Q54 |  |  | | How many internal-only servers are in scope for engagement? | See response to Q50. |
| Q55 |  |  | | How many external-facing servers are in scope for the engagement? | ~40. |
| Q56 |  |  | | How many applications are in-scope for the engagement | Approximately 11. |
| Q57 |  |  | | Please describe the details for the in-scope applications. | The systems that are in scope manage insurance benefits, enrollments, life events, payments of premiums, invoicing, demographic information, authentication and authorization, and integrations between these different systems. |
| Q58 |  |  | | How many users are in-scope for the engagement? | About 400. |
| Q59 |  |  | | Please describe the technical environment of your organization. | See response to Q39 |
| Q60 |  |  | | Please describe the security solutions and controls of your organization. | See response to Q29. |
| Q61 | Section 5.1 | 19 | | Can you describe in high level the existent cybersecurity/IT team for the Department? | ETF’s cybersecurity and IT teams are responsible for identifying, protecting, detecting, responding and recovering from cyberthreats to ETF assets. |
| Q62 | Section 5.1 | 19 | | Is the Department following any certain IT standards as outlined in the RFP? | NIST standards. |
| Q63 | Section 5.1 | 20 | | Are presentations for engagement results to be delivered in person or virtually? | Presentation can be delivered virtually. |
| Q64 |  |  | | What is the anticipated budget? | The Department chooses not to answer this question. |
| Q65 |  |  | | How many estimated live internet-exposed resources are in-scope, such as servers, VPN gateways, websites, and firewalls? | See response to Q10. |
| Q66 |  |  | | How many estimated internal hosts are in-scope, such as computers and servers? | See response to Q10. |
| Q67 |  |  | | How many wireless networks are in-scope for testing? | One. |
| Q68 |  |  | | For Wireless Network Penetration Test   1. How many wireless networks are in-scope for testing? 2. Can all wireless networks be reached from one location? If not, how many locations need testing? | One. |
| Q69 |  |  | | For Web Application Penetration Test   1. How many web applications are in-scope for testing? 2. Please list the URL for each in-scope web application: 3. How many sets of credentials are to be tested for each application? 4. How many estimated dynamic pages does each application contain? 5. Are there calls to your own API(s) made by the application(s) that are in-scope for testing? If so, how many estimated API calls are in-scope for each application? | See response to Q15. |
| Q70 |  |  | | For Web Application Penetration Test   1. How many web applications are in-scope for testing? 2. Please list the URL for each in-scope web application: 3. How many sets of credentials are to be tested for each application? 4. How many estimated dynamic pages does each application contain? 5. Are there calls to your own API(s) made by the application(s) that are in-scope for testing? If so, how many estimated API calls are in-scope for each application? | See response to Q69. |
| Q71 |  |  | | For Phishing / Social Engineering Work   1. Do you want us to perform Email Phishing, where we send various phishing emails to your users? If so, how many estimated users are to be tested? 2. Do you want us to perform SMS Phishing, where we send phishing text messages to your users? If so, how many estimated users are to be tested? 3. Do you want us to perform Phone Phishing, where we call your users/numbers and attempt to elicit sensitive information? If so, how many estimated users are to be tested? 4. Do you want us to perform On-Site Social Engineering, where we visit your facility/office and attempt to bypass security measures and gain access to the facility and/or internal network? If so, please list each location to be tested. | 1. Yes, about 400. 2. No. 3. Yes, about one. 4. Yes, one. |
| Q72 |  |  | | Are there any constraints during testing?   1. Time of day 2. Critical IPs that must not be disrupted 3. Network traffic limits | Yes, there may be constraints. Depending on the test/activities being performed, the Department may need to limit traffic during business hours or critical processing times. This will be worked out prior to the given test or activity. |
| Q73 |  |  | | How many public IP addresses and public domain names are there? | Approximately 40 public external – <4 top level domains |
| Q74 |  |  | | What critical devices must not be disrupted? | That can be discussed later. |
| Q75 |  |  | | Scope   1. How many databases are to be reviewed? 2. What kind of databases are to be reviewed? 3. Is there any public policy or framework that this needs compliance against? 4. Do you have any internal policies that this needs compliance against? | 1. 5-10.  2. SQL Server, DB2.  3. HIPAA compliance with §164.308(a)(1)(ii).  4. IRMP – data classification, acceptable use. |
| Q76 |  |  | | Backup/Restore/Disaster Recovery  Constraints   1. Which services need to be reviewed? 2. Is there any public policy or framework that this needs compliance against? 3. Do you have any internal policies that this needs compliance against? | The Department has existing procedures for these activities. The goal is to ensure existing procedures are sufficient to meet recovery needs. |
| Q77 |  |  | | Social Engineering  Scope   1. What types of attacks are you looking for?    1. Phishing?    2. Vishing?    3. Something else? 2. How many email addresses/people are in scope? | See response to Q71. |
| Q78 |  |  | | Assumed Breach Testing/Red Team Operation  Scope   1. Which networks are in scope? 2. How long should this operation last?   Constraints   1. Are our hours of operation restricted? | 1. Internal and external. 2. With-in two weeks. This will be coordinated with ETF during the engagement. 3. During core business hours (8-5). |
| Q79 |  |  | | Cloud Services Testing  Scope   1. Which SharePoint environments are in scope? 2. Which OneDrive folders are in scope? 3. Which Exchange environments are in scope? | For penetration testing these systems would be in scope. |
| Q80 |  |  | | Are there any concerns with SDLC? | Goal is to ensure existing policies and procedures are being followed and that the existing processes meet industry best practices. |
| Q81 |  |  | | What’s the perspective of the evaluation? Security focused? Best practice? User? | Ensuring industry best practices for security, compliance (NIST), and proper processes and procedures are in place. |
| Q82 | Section 8.1 | 22-23 | | How many servers and workstations are considered in-scope for the security assessment? | See response to Q10. |
| Q83 | Section 8.1 | 22-23 | | How many active end-users are considered in-scope for the security assessment? | ~400. |
| Q84 | Section 8.1 | 22-23 | | How many web applications are considered in-scope for reviewing the security of the SDLC? | Less than 10. |
| Q85 | Section 8.1 | 22-23 | | How many physical sites are considered in-scope for the physical security assessment? | One. |
| Q86 | Appendix 2 – Technical Questionnaire |  | | How many devices/assets are in the environment? | See response to Q10. |
| Q87 | Appendix 2 – Technical Questionnaire |  | | What device types are within the environment? | Standard office setting devices, e.g., laptops, printers, servers, etc. |
| Q88 | Appendix 2 – Technical Questionnaire |  | | Will the contractor be permitted to perform vulnerability scans remotely or onsite? Or would the Contractor be required to utilize the Departments vulnerability tools. | Remote is fine. Contractor may use their tools, but more detailed discussions would take place before the exercise would be executed. |
| Q89 | Appendix 2 – Technical Questionnaire |  | | How many employees are within the department? | About 400. |
| Q90 | Appendix 2 – Technical Questionnaire |  | | For physical social engineering, how many sites would be included? | One. |
| Q91 | Appendix 2– Technical Questionnaire |  | | How many data centers and locations are in scope? | One. |
| Q92 | RFP Section 2.5 Uploading Documents to BOX | 14 | | When opened, the linked URL for BOX that’s on pg. 14 displays a message that the page is unavailable/been moved. Is there a different link in BOX for uploading our proposal documents? | Please see the Department’s website for this procurement at <https://etf.wi.gov/node/38681> where the BOX URL is listed. If problems persist, email [ETFSMBProcurement@etf.wi.gov](mailto:ETFSMBProcurement@etf.wi.gov). |
| Q93 | RFP Section #5.1.A FY25 (July 1, 2024 – June 30, 2025) | 19 | | Is the onboarding and offboarding process centralized? | Yes. |
| Q94 | RFP Section #5.1.A FY25 (July 1, 2024 – June 30, 2025) | 19 | | Would you like us to also evaluate the process for changing existing access rights? And internal transfers? | Yes. |
| Q95 | RFP Section #5.1.A FY25 (July 1, 2024 – June 30, 2025): | 19 | | Would you like us to also evaluate the process for Contractor access? | Yes. |
| Q96 | RFP Section #5.1.A FY25 (July 1, 2024 – June 30, 2025) | 19 | | Is the penetration testing and vulnerability assessment focused on the network and not applications, similar to 2019? | Yes, the network and applications will be in scope. |
| Q97 | RFP Section #5.1.A FY25 (July 1, 2024 – June 30, 2025): | 19 | | EXTERNAL penetration testing: how many external facing IP addresses do you have? | ~40. |
| Q98 | RFP Section #5.1.A FY25 (July 1, 2024 – June 30, 2025) | 19 | | INTERNAL penetration testing: how many internal IP addresses do you have? | See responses to Q9, Q36 and Q27. |
| Q99 | RFP Section #5.1.A FY25 (July 1, 2024 – June 30, 2025) | 19 | | How many wireless networks are in scope? | One. |
| Q100 | RFP Section #5.1.A FY25 (July 1, 2024 – June 30, 2025) | 19 | | Do you have an existing IT Audit risk assessment methodology that we should follow? | Please refer to Appendix B of the [Biennial Audit Plan](https://etf.wi.gov/boards/audit/2023/06/22/aud7a/download?inline=) for the risk assessment methodology. The inherent risk is assessed based on its impact and likelihood. The assessment of internal control effectiveness is used to determine the residual risk. |
| Q101 | RFP Section #5.1.A FY25 (July 1, 2024 – June 30, 2025) | 19 | | Do you have an existing IT Audit plan template that we should utilize? | Following the existing template is not required. |
| Q102 | RFP Section #5.1.B. FY26 (July 1, 2025 – June 30, 2026) | 19 | | How many system integrations do you have currently?  Will a sampling approach be acceptable for testing this area? | About 5 – 10. Yes, sampling would be acceptable. |
| Q103 | RFP Section #5.1.B. FY26 (July 1, 2025 – June 30, 2026) | 19 | | Is the SDLC process centralized and the same for all application environments? | Yes. |
| Q104 | Appendix 3, Section 3.0 (Legal Relations) | 1 | | Will the Department exclude any losses arising from the acts or omissions of the Department from the indemnification below.  Proposer cannot:  “The Contractor accepts full liability and agrees to hold harmless the State, the Department’s governing boards, the Department, its employees, agents and contractors for any act or omission of the Contractor, or any of its employees, in connection with the Contract, **except to extent such liability arose from the acts or omissions of the Department.**” | ETF will consider this edit during contract negotiations. |
| Q105 | N/A | N/A | | Does the department have an annual budget set for this work that can be shared? | The Department chooses not to answer this question. |
| Q106 | N/A | N/A | | Does the Department have a internal audit methodology with required templates and reports to follow or would you prefer to use ours? | The Department is open to using the Contractor’s methodology/templates. |
| Q107 | 5.1 Services, subsection A FY25 (July 1, 2024 – June 30, 2025), Subsection i Assess onboarding and offboarding process | 19 | | Is there more than one process to be reviewed? For example, each entity or application system, etc. has its own process. | There is a standard process for onboarding and offboarding. Applying access to applications can vary depending on the application. The Contractor will review the processes/procedures to ensure established processes are being followed and that they meet industry best practices. |
| Q108 | 5.1 Services, subsection A FY25 (July 1, 2024 – June 30, 2025), Subsection i Assess onboarding and offboarding process | 19 | | Does the department use an identity and access management system to automate the on-boarding/off-boarding process? | No. |
| Q109 | 5.1 Services, subsection A FY25 (July 1, 2024 – June 30, 2025), Subsection i Assess onboarding and offboarding process | 19 | | Have standard access roles been defined and implemented for all users? | Yes. |
| Q110 | 5.1 Services, subsection A FY25 (July 1, 2024 – June 30, 2025), Subsection i Assess onboarding and offboarding process | 19 | | What is the size of the user population? | ~400. |
| Q111 | 5.1 Services, subsection A FY25 (July 1, 2024 – June 30, 2025), Subsection i Assess onboarding and offboarding process | 19 | | How many different IT environments (e.g. Windows, Unix, etc.) | The onboarding and offboarding audit will be include evaluation of existing processes and procedures and isn’t unique to Windows or Unix/Linux. It’s ensuring existing processes and procedures are being followed and meet industry best practices. |
| Q112 | 5.1 Services, subsection A FY25 (July 1, 2024 – June 30, 2025), Subsection i Assess onboarding and offboarding process | 19 | | How many different application systems? | ~20. |
| Q113 | 5.1 Services, subsection A FY25 (July 1, 2024 – June 30, 2025), Subsection i Assess onboarding and offboarding process | 19 | | Is on-boarding/off-boarding limited to department staff or are external users included, such as WRS members. | External users, such as WRS members are not in scope. |
| Q114 | 5.1 Services, subsection A FY25 (July 1, 2024 – June 30, 2025), Subsection ii Conduct penetration testing and vulnerability assessment | 19 | | How many external IP addresses (public IPs) do you own? | See response to Q36. |
| Q115 | 5.1 Services, subsection A FY25 (July 1, 2024 – June 30, 2025), Subsection ii Conduct penetration testing and vulnerability assessment | 19 | | How many custom-developed or customized off-the-shelf Internet-facing web applications are living on your IPs and in scope for testing? | < 20. See response to Q9. |
| Q116 | 5.1 Services, subsection A FY25 (July 1, 2024 – June 30, 2025), Subsection ii Conduct penetration testing and vulnerability assessment | 19 | | How many internal network segments (VLANs) do you have? | 57 VLANs. |
| Q117 | 5.1 Services, subsection A FY25 (July 1, 2024 – June 30, 2025), Subsection ii Conduct penetration testing and vulnerability assessment | 19 | | How many locations are included in wireless testing? | One. |
| Q118 | 5.1 Services, subsection A FY25 (July 1, 2024 – June 30, 2025), Subsection iii Develop IT audit plan | 19 | | Given the standards listed, we would recommend adding:  • Also include NIST Cybersecurity Framework.  • Given privacy concerns, does the department need to include risks and regulatory requirements of HIPAA, and/or other privacy regulations/  Would this be of interest? | Yes. |
| Q119 | 5.1 Services, subsection B FY26 (July 1, 2025 – June 30, 2026), Subsection i Perform system integration audit | 19 | | How many application systems are included in the scope of this review? | See response to Q84. |
| Q120 | 5.1 Services, subsection B FY26 (July 1, 2025 – June 30, 2026), Subsection i Perform system integration audit | 19 | | How many separate integrations are there among these application systems? | See responses to Q102 and Q43. |
| Q121 | 5.1 Services, subsection B FY26 (July 1, 2025 – June 30, 2026), Subsection ii Conduct system development life cycle audit | 19 | | Does the department follow a DevOps/DevSecOps model for development? | The Department is just now beginning to incorporate more DevOps principles into our SDLC workflow. |
| Q122 | 5.1 Services, subsection B FY26 (July 1, 2025 – June 30, 2026), Subsection ii Conduct system development life cycle audit | 19 | | Does the department employ any development tools to manage SDLC? | The Department primarily uses Ivanti and Jira to manage SDLC processes from a workflow perspective. On the technical side, the Department uses actions in GitHub to handle things like code reviews/quality checks and deployments. |
| Q123 | 5.1 Services, subsection B FY26 (July 1, 2025 – June 30, 2026), Subsection iii Perform disaster recovery audit | 19 | | Prior to the audit, has any disaster plan testing been performed - - either simulated disasters and live testing of the plan or tabletop walk throughs? | Yes, the Department does annual exercises. |
| Q124 | 5.1 Services, subsection B FY26 (July 1, 2025 – June 30, 2026), Subsection iii Perform disaster recovery audit | 19 | | Has the department performed a business impact analysis to define IT disaster plans? | Yes. The Department has a Continuity of Operations Plan (COOP) team that works with each business area to define an impact analysis unique to their business needs. |
| Q125 | N/A | N/A | | How much of the intended work will be onsite versus remote? | Mostly remote, except for the social engineering testing. |
| Q126 | Section 5.1.A(ii) | | 19 | Does the Wisconsin Department of Employee Trust Funds desire "internal" and "external" penetration testing and vulnerability assessments? | Both. |
| Q127 | Section 5.1.A(ii) | | 19 | How many external IP addresses are in scope for the external penetration test and vulnerability assessment? | ~40. |
| Q128 | Section 5.1.A(ii) | | 19 | How many internal IP addresses and/or endpoints are in scope for the internal penetration test and vulnerability assessment? | See response to Q10. |
| Q129 | Section 5.1A(ii) | | 19 | For the physical social engineering test, do you want this inclusive of phishing and vishing testing? Or do you want it specifically focused toward onsite social engineering techniques? | Yes. |
| Q130 | Section 5.1.A(ii) | | 19 | Are there any dates and times that the penetration and vulnerability tests need to be performed or that these tests should not be performed or avoided? | Dates and times will be coordinated with the Contractor at a later time. |
| Q131 | Section 5.2.A(iii) | | 19 | For the audit year 2025-2026, there is direct mention of the "insurance administration" system being in scope. Is that the core system that all of these workstreams will be focused on or is that specific to the disaster recovery audit workstream? | It is specific to the disaster recovery engagement. |
| Q132 | Section 5.1.A(i) | | 19 | Are the onboarding and offboarding activities that will be assessed managed centrally by an individual office or are the management of these activities disbursed across a variety of personnel/ offices? | Centralized. |
| Q133 | Section 5.1.A(iii) | | 19 | Is there an expectation that the IT audit plan developed in FY25 could alter or inform the three FY26 audits described in the RFP? | Yes. |
| Q134 | Section 5.1.A(iii) | | 19 | With regard to the standards listed, does the Department have a preference for which standard is utilized? | NIST 800 series. |
| Q135 | Section 5.1.B(ii) | | 19 | This paragraph references the “sample system”. Can you provide a background or description of this system? | See response to Q57. |
| Q136 | Section 5.1.B(iii) | | 19 | To what degree is the Department’s disaster recovery plan dependent upon external resources and infrastructure (e.g., state or commercial provider)? | The Department is dependent on the State data center, integration vendors’ data centers, and the Department’s SaaS vendor. |
| Q137 | 5.1 Services  A FY25 (July1, 2024 – June 30, 2025) | | 19 | Is the onboarding/offboarding process homogenous across all systems? | It’s centralized to one team, but the process for managing access will vary depending on the specific systems/applications. There are approx. 20 different applications where access is given. |
| Q138 | 5.1 Services  A FY25 (July1, 2024 – June 30, 2025) | | 19 | If the onboarding/offboarding process is not homogenous, can you provide an estimate of how many different processes and teams are involved in onboarding and offboarding users. | See response to Q137. |
| Q139 | 5.1 Services  A FY25 (July1, 2024 – June 30, 2025) | | 19 | Can you share the breakout of how many systems are on premise vs. cloud based? | On prem: ~10; Cloud: 2; Saas: 2. |
| Q140 | 5.1 Services  A FY25 (July1, 2024 – June 30, 2025) | | 19 | Approximately how many IP addresses and ranges would be in scope for the penetration test? | See response to Q57 |
| Q141 | 5.1 Services  A FY25 (July1, 2024 – June 30, 2025) | | 19 | Is the Management of any part of the network outsourced? | The network is managed by the State’s Department of Administration / Division of Enterprise Technology. |
| Q142 | 5.1 Services  A FY25 (July1, 2024 – June 30, 2025) | | 19 | Is the expectation that penetration testing includes an external assessment, internal assessment or both? | Both. |
| Q143 | 5.1 Services  A FY25 (July1, 2024 – June 30, 2025) | | 19 | How many internal systems are in scope for an internal assessment? | Approximately 25. |
| Q144 | 5.1 Services  A FY25 (July1, 2024 – June 30, 2025) | | 19 | How many domains is your network comprised of? | 1 primary and < 5 sub domains. |
| Q145 | 5.1 Services | | 19 | How many users are there in your network environment?  [We understand a variation of this question was asked as part of the 2019 RFP, however we are looking to understand if anything has changed since then]. | ~400. |
| Q146 | 5.1 Services  A FY25 (July1, 2024 – June 30, 2025) | | 19 | Is there segmentation between the sites or is it a flat network? | Yes, there is network segmentation. |
| Q147 | 5.1 Services | | 19 | Do you anticipate including an assessment of your wireless network? | Yes. |
| Q148 | 5.1 Services  A FY25 (July1, 2024 – June 30, 2025) | | 19 | Do you anticipate including an assessment of any cloud infrastructure (if applicable)? | Yes, but testing would be that of access control appropriateness and not vulnerability of the Department cloud service providers’ applications. |
| Q149 | 5.1 Services | | 19 | How many physical locations would be in scope for the penetration testing and vulnerability assessment procedures? | One. |
| Q150 | 5.1 Services  A FY25 (July1, 2024 – June 30, 2025) | | 19 | In addition to physical social engineering, would you anticipate including telephonic or electronic social engineering as part of this scope? | Yes. |
| Q151 | 5.1 Services  A FY25 (July1, 2024 – June 30, 2025) | | 19 | Do you anticipate including a Web application assessment within the scope of the penetration testing? | Yes. |
| Q152 | 5.1 Services  A FY25 (July1, 2024 – June 30, 2025) | | 19 | Is there a targeted minimum number of audits that the organization anticipates being completed during each fiscal year? | The Department’s goal is to complete the audits as planned, but the audit plan is subject to change. |
| Q153 | 5.1 Services  B FY26 (July1, 2025 – June 30, 2026) | | 19 | Regarding the scope of the system integration audit, how many systems are anticipated to be in scope for this audit? | About 11. |
| Q154 | 5.1 Services  B FY26 (July1, 2025 – June 30, 2026) | | 19 | How many systems are developed in-house vs. are third party applications? | In scope for this project there are less than 10 in-house developed applications, and about 5 third-party applications. |
| Q155 | 5.1 Services  B FY26 (July1, 2025 – June 30, 2026) | | 19 | Is there comprehensive current state system documentation for systems anticipated to be in scope for the system integration audit? | There is some documentation, but it is not comprehensive. |
| Q156 | 5.1 Services  B FY26 (July1, 2025 – June 30, 2026) | |  | Is there a formal documented system development life cycle (SDLC) methodology currently in place? | Yes. |
| Q157 | 5.1 Services  B FY26 (July1, 2025 – June 30, 2026) | |  | Is there an anticipated number of sampled projects that would be expected to be evaluated as part of the SDLC audit? | The Department expects the audit to evaluate and validate the Department’s existing SDLC processes and procedures. This could be done against 2 – 3 sample developments projects/initiatives. |
| Q158 | 5.1 Services  B FY26 (July1, 2025 – June 30, 2026) | |  | Has the organization performed a BIA assessment in recent years? If so, when was this last performed? | It’s performed annually. |
| Q159 | 5.1 Services  B FY26 (July1, 2025 – June 30, 2026) | |  | Are there current DR policies and procedures in place? | Yes. |
| Q160 | 5.1 Services  B FY26 (July1, 2025 – June 30, 2026) | |  | How many data centers does the organization operate / rely on for DR?  [We understand a variation of this question was asked as part of the 2019 RFP, however we are looking to understand if anything has changed since then]. | The State has 2 data centers. The Department relies on its vendors and their DR operations to meet established SLA’s and guarantees. |
| Q161 | 5.1 Services  B FY26 (July1, 2025 – June 30, 2026) | |  | Are there any specific regulatory requirements we should be aware of related to disaster recovery?  [We understand a variation of this question was asked as part of the 2019 RFP, however we are looking to understand if anything has changed since then]. | No. |
| Q162 | 5.1 Services  B FY26 (July1, 2025 – June 30, 2026) | |  | Do you utilize cloud services in relation to DR? | No. |
| Q163 | 5.1.A | | 19 | What is the average population of new hires per year? | In the last two fiscal years, approximately 95 per year on average. |
| Q164 | 5.1.A | | 19 | What is the average population of terminations per year? | In the last two fiscal years, approximately 74 per year on average. |
| Q165 | 5.1.A | | 19 | How many IP addresses are in-scope for the vulnerability assessment and penetration test? (Please provide both external and internal) | See responses to Q10, Q36, Q53, Q97, Q98, Q127, Q128, Q140. |
| Q166 | 5.1.A | | 19 | What level of vulnerability testing is expected? (Network layer, application layer, database layer) | Yes, to each example in the question. Network, App, & Data, but should include social as well as process exploitation. |
| Q167 | 5.1.A | | 19 | Are there any excluded IP addresses in the vulnerability assessment and penetration test? | Yes. Details will be discussed prior to the engagement. |
| Q168 | 5.1.B | | 19 | How many systems will be included in the system integration audit? | About 10. |
| Q169 | 5.1.B | | 19 | How many applications will be included in the SDLC audit? | < 10. |
| Q170 | 5.1.B | | 19 | For the DR audit, the only application referenced is the insurance administration system. Does this audit include other applications or just focused on the application mentioned? | The Insurance Administration System includes about 10-11 applications. |
| Q171 | 5.1.A and 5.1.B | | 19 | Can you provide the number of hours spent on audits listed in the RFP from prior year? | Prior hours are not a good reference as engagements / engagement scopes could be very different. |
| Q172 | 5.1.A and 5.1.B | | 19 | Is there a range of hours you anticipate for this RFP? | The Department is unable to answer this question. |
| Q173 | 5.1 | | 19 | For FY26 service i, can the Department provide the number of systems to be evaluated? | About 10-11. |
| Q174 | 5.1 | | 19 | Will the deliverables provided to ETF be shared with third parties as part of ETFs reporting requirements? For example, DOA/DET, Legislative Audit Bureau, federal agencies, etc. | Reports may be shared with oversight boards and committees along with the State’s Legislative Audit Bureau (LAB). |
| Q175 | 5.1 | | 19 | What framework(s) does the Department aim to follow? Please include all that are applicable from a cybersecurity perspective. | Security controls are NIST 800 series while policies are written to ISO 27001. |
| Q176 | 5.1 | | 19 | Are there any existing tools that are procured by the state that will be utilized for penetration testing? | No. |
| Q177 | 5.1 A and B | | 19 | Are there a preferred testing windows for FY25 and FY26? If so, when? | No preference determined at this time, but will be jointly planned by both parties. |
| Q178 | 5.1 A and B | | 19 | Are there preferred report dates for each work phase? If so, when? | Upon completion, reports to internal stakeholders, then to the Audit Committee at its upcoming quarterly meetings. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Q179 | 5.1 A.i FY 25 On Boarding/Off boarding | 19 | Approximately how many new hires/separations are anticipated during the period (historic averages are fine)? | See responses to Q163 and A164. |
| Q180 | 5.1 A.i FY 25 On Boarding/Off boarding | 19 | How many internal personnel are expected to participate in interviews? | Between 10 and 20. |
| Q181 | 5.1 A.i FY 25 On Boarding/Off boarding | 19 | How many systems will we need to review for appropriate access removal? | 10 – 20. |
| Q182 | 5.1 A.i FY 25 On Boarding/Off boarding | 19 | Is sample testing adequate (e.g. sampling a number of new hire and terminations to see if the process completed correctly), or do you want full population/substantive tests completed? | Sample testing is what’s expected. |
| Q183 | 5.1 A.ii Vulnerability Scanning | 19 | How many IP addresses will need to be included in the scans? | See response to Q13. |
| Q184 | 5.1 A.ii Vulnerability Scanning | 19 | How will access to the environment be facilitated for the scan, to deploy the scanning tools? | External scan can happen via the web, for internal scans network access will be granted. |
| Q185 | 5.1 A.ii Vulnerability Scanning | 19 | Of the IPs included in-scope, how many are publicly facing, and how many are internal-only? | Approximately 40 external,  120 internal only. |
| Q186 | 5.1 A.ii Penetration testing | 19 | How many discrete web applications are in-scope for the penetration test (how many web-based authentication instances are there)? | About 10 web applications with 3 authentication instances. |
| Q187 | 5.1 A.ii Penetration testing | 19 | Is API testing required, and if so, how many APIs, what type are they (Graph, REST, etc.), and are there test files (e.g. postman) available for use? | The Department has 12 REST APIs built and deployed in the AnyPoint platform, and one GraphQL API (with a Java REST wrapper) deployed on the Department’s web application platform. |
| Q188 | 5.1 A.ii Penetration testing | 19 | Is physical penetration testing required? If so, how many sites? | Yes to one site. |
| Q189 | 5.1 A.ii Penetration testing | 19 | Is network penetration testing required?  If yes, how many external network entry points need to be tested (e.g. VPN endpoints, etc.)? | Yes. 4 VPN, Internet / Web, internal and physical wireless networks. |
| Q190 | 5.1 A.ii Social Engineering | 19 | How many individuals will be covered by the social engineering test? | Yes, 400 employees for a generic campaign and 30 or so for a targeted crafted campaign. |
| Q191 | 5.1 A.iii IT Audit Plan | 19 | Has a cybersecurity framework been adopted and implemented? If yes, which framework? | See response to Q175. |
| Q192 | 5.1 A.iii IT Audit Plan | 19 | Does the IT audit cover all the same systems included in the vulnerability scan and pen test? | Yes. |
| Q193 | 5.1 A.iii IT Audit Plan | 19 | If not, how many systems are included in the test, and are any hosted on-premises? | See above. |
| Q194 | 5.1 A.iii IT Audit Plan | 19 | If we use the CIS Critical Security Controls as the control baseline, is there a specific Implementation Group (1-3) that we should plan to audit against? | Implementation Group 3. |
| Q195 | 5.1 B.i FY26 System Integration Audit | 19 | How many systems/system connections will need to be reviewed? | About 10 systems. |
| Q196 | 5.1 B.i FY26 System Integration Audit | 19 | Are these on-premises, colocation hosted, cloud-hosted (within an internal cloud account), or SaaS-delivered systems? Can we get rough approximations of each? | See response to Q139. |
| Q197 | 5.1 B.i FY26 System Integration Audit | 19 | Which/how many specific data elements need to be included in the audit (e.g. payroll expense, retirement benefit payouts, ePHI from insurance claims, etc.)? | This doesn’t seem to be relevant to the scope of the audit. |
| Q198 | 5.1 B.i FY26 System Integration Audit | 19 | Are there specific reports that need to be validated, and if so, how many? | Unknown at this time. |
| Q199 | 5.1 B.ii SDLC Audit | 19 | Has the Department implemented a specific development methodology, and if so, what (e.g. agile development, DevOps, traditional waterfall, etc.)? | Hybrid Agile and waterfall. Depends on the project and development work being done. |
| Q200 | 5.1 B.ii SDLC Audit | 19 | How many in-house developed systems are in-scope? | See response to Q154. |
| Q201 | 5.1 B.ii SDLC Audit | 19 | How large is the development/engineering team(s)? | Approximately 30. |
| Q202 | 5.1 B.iii Disaster recovery Audit | 19 | Are the existing contingency and recovery plans Department-wide? Or are there specific plans for different groups/teams within the Department? | Each business area is responsible for developing their own plans. |
| Q203 | 5.1 B.iii Disaster recovery Audit | 19 | Is the audit solely focused on the insurance administration system, or are there others ancillary systems that will need to be included as well (e.g. an Active Directory Domain Controller)? | The focus of the audit is on the Insurance Administration System and other systems that it is dependent on. |