SAN DIEGO CITY EMPLOYEES' RETIREMENT SYSTEM ("SDCERS")

Request for Proposals ("RFP") for IT Internal Auditing Services
Questions Received from Firms
September 13, 2019

INTERNAL AND EXTERNAL NETWORK PENETRATION AUDIT RELATED QUESTIONS

1. External Penetration Test:
   a. How many live external IP addresses? *12*

2. Internal Penetration Test:
   a. How many systems, desktops, laptops, IPs are in scope? *255*
   b. Can testing be performed remote using devices? *Potentially, if the City of San Diego and SDCERS firewalls do not block the remote devices.*
   c. What are preferred testing times? *6pm-6am.*

3. Web Application Testing:
   a. How many web applications are to be tested? *Clarification*: *Web application testing is out of scope; web application/website penetration testing is already performed on critical web applications by an outside vendor. Please refer to the original RFP Section titled "External Penetration Testing."* ***Scope of this RFP only includes evaluation of a sample of the outside vendor's results. Tests occur 12 times per year, minimum.***
   b. How many dynamic pages per application? *See Question #3a above.*
   c. How many authenticated user roles per application? *See Question #3a above.*

4. Please provide the following for the Internal and External Network Penetration testing audit:
   a. How many critical applications are there? *The pension administration software is the most critical application, but two other critical applications are in scope.*
   b. The RFP states that the tester will act as an unauthorized user, but will the tester also be unauthenticated? *Yes.*
   c. The IP address in scope for external network penetration testing? *Actual IP addresses will be provided to the awardee.*
   d. Number of websites in scope. *See Question #3a above.*
   e. Number of assets in scope for internal network penetration testing. *See Question #2a above.*
      i. *Are digital printers and fax machines (if used) in scope? Yes.*
   f. Are wireless access points in scope for internal network penetration testing? *SDCERS does not have wireless access points.*
   g. Does SDCERS have any unstable or unsupported systems that will be part of the scope? *No.*
   h. Are there any web applications to be tested as part of this scope? If yes, please provide the following: *See answer to Question #3a above.*
      i. *On average, how many static pages are available on the site prior to authentication?*
      ii. *On average, how many dynamic pages are available on the site prior to authentication?*

iii. *On average, how many forms (including hidden forms) are available on the site prior to authentication?*
iv. *On average, how many static pages are available on the site post- authentication?*
v. *On average, how many dynamic pages are available on the site post- authentication?*
vi. *On average, how many forms (including hidden forms) are available on the site post-authentication?*

i. Would you prefer the penetration testing audit to be performed as a black-box test or will access credentials and selected information about the environment be provided? *A range of IPs will be provided.*

5. For the Penetration Testing:
   a. Have scans/tests been performed in the past? *Yes. Nessus scans are performed weekly, Department of Homeland Security scans are performed weekly and website penetration tests are performed monthly (at a minimum).*
   b. How many IP addresses are in scope? *See answer to Question #1a and #2a above.*
   c. Will it be a gray-box test? *A range of IPs will be provided.*

6. How many internal IP addresses are in scope? *See answer to Question #2a above.*

7. How many external IP addresses are in scope? *See answer to Question #1a above.*

8. For Penetration Test:
   a. Breach the organization by acting as an unauthorized user, with the ultimate goal of compromising your networks and data.
      i. Are any attacks off limits? *DoS (Denial of Service).*
      ii. Are you interested in a report to show where and when of the test? *Yes.*
      iii. What systems what time? *Yes, we want to know what systems at what times.*
   b. The tests seek to exploit weaknesses in systems. Obtain access to sensitive data and systems.
      i. Do you have systems that are not in scope? *Limit scope to key systems identified.*
      ii. Do you want any data removed or added? *No.*
   c. Gain administrative access over the network.
      i. Do you want us to pinpoint when we have access? *Yes.*
      ii. Do key stakeholders know there is testing? *CIO, so we don't expend resources as we would for a real event.*
      iii. Will your MSP be alerted to test times? *No.*
   d. Determine the ability of an attacker to exfiltrate data undetected outside of the network.
      i. At what point should we notify your team? *When all vulnerabilities are identified.*
      ii. Are you looking for physical and social engineering? *No.*
   e. Identify critical application vulnerabilities on externally facing applications.
      i. How many applications? *See answer to Question #3a above.*
      ii. How many are cloud based? *See answer to Question #3a above.*

9. For each web application: *See answer to Question #3a above.*
   a. The URL/IP address if publically accessible.

i. If not how are the applications accessed?

b. A brief summary on what the application is used for.
c. What functionality exists before login, and approximate number of pages (e.g. login, register, forgotten password)?
d. What functionality exists after login, and approximate number of pages (e.g. add to basket, payment, write blog post, account management – change password)?
e. How many user roles are there, and what levels of privilege do they have?
f. Where is the application hosted (cloud etc.)?
g. Which programming language(s) is the application written in?
h. Which platform(s) is the web server running?

10. For web services:
    a. How many web service endpoints are there in scope? *12*
    b. What are the number of functions per web service? *Variable.*
    c. Is the Web Service specification/documentation available for scoping and/or testing purposes? *Yes.*
    d. What technology are the web services using? (e.g. SOAP/RESTFUL) *IIS.*
    e. Do the web services require authentication? *Yes.*

11. External Infrastructure
    a. Number of active Internet facing IP addresses *12*
    b. Types of publically accessible services (e.g. FTP, SFTP, SMTP) *SFTP, SMTP, WWW.*

12. For Internal Infrastructure:
    a. Number of workstations? *100*
    b. Number of servers? *110*
    c. Which operating systems are in use? *Windows.*
    d. Is the network segmented or flat? *Segmented.*
        i. Can all networks/VLANs in scope be accessed from one network point? *Yes.*
        ii. Number of networks/VLANs in scope? *3*
    e. Is there any Wireless capability? *See answer to Question #4f above.*
        i. Number of Access Points?
        ii. Number of SSIDs broadcasted?
        iii. What types of authentication are in use, if any?
    f. Where is geographical location of the internal environment? *On site*
        i. If there are multiple sites, where are the locations for each? *San Diego*
        ii. Can all locations be accessed from one main site? *Yes.*

13. Firewall Review/Rulebase Review
    a. Number of Firewalls including brands *2 Cisco Firewalls.*
    b. Is the requirement for a full firewall configuration review and/or a rulebase review? *No.*
    c. Number of rules per rulebase/firewall *N/A.*

14. Social Engineering – Remote: *See answer to Question #8dii above – not in scope.*

a. Number of Staff
b. Details of any corporate remote access systems e.g. Outlook Web Access, SSL VPN etc.

15. Social Engineering – Onsite: *See answer to Question #8dii above – not in scope.*
    a. Number of Geographical Locations
    b. Number of staff per location
    c. Number of devices per location
    d. Are the locations within a shared office environment?

16. Mobile Applications: *Mobile applications not in scope at this time.*
    a. What platform(s) is the application written for? e.g. iOS/Android
    b. How are the applications accessed (are they available on their respective app stores)?
    c. A brief summary on what the application is used for.
    d. What functionality exists pre-authentication, and approximate number of pages (if it's just a login form then that's fine)?
    e. What functionality exists post-authentication, and approximate number of pages (e.g. file upload, download, search, database queries)?
    f. How many user roles are there, and what levels of privilege do they have?

ITGC AUDIT RELATED QUESTIONS

17. Please confirm if there are additional applications in scope for the ITGC audit beyond the 3 applications mentioned– pension administration software, accounting software, and document management software. *These are the only three applications, but supporting infrastructure for these three applications and Active Directory are in scope as well.*
    a. Is the above-mentioned software located on premises at SDCERS' data center, or are they all hosted/cloud-based applications? *On premise.*
    b. If on-premises, what is their architecture (web-based, client-server, mainframe, etc.)? *In-scope applications: IRIS web-based; Dynamics GP client-server; Documentum web-based.*
        i. *Please provide information on their operating systems and back-end databases. All systems run on Windows 12 R2 servers with SQL 2014 R2 databases.*

18. How many Applications? *See answer to Question #17 above.*

19. Is SDCERS following Secure Development Lifecycle within 'Software Development and Change Management process'? *SDCERS follows the Agile SDLC process.*

20. What are the SDCERs environments hosted (e.g. office, cloud, data center)? *See answer to Question #17a above.*

21. Have you had an IT General Controls Audit? *SDCERS has not had an ITGC Internal Audit performed.*

OPERATING EFFECTIVENESS OF 2017 SECURITY RISK ASSESSMENT REMEDIATION RELATED QUESTIONS

22. For the Operating Effectiveness of 2017 Security Risk Assessment Remediation audit:
    a. How many findings were identified? Were the findings categorized with any criticality rankings (H, M, L)? *19 security findings. These findings were mapped to 15 security risks, four which were considered high, eight which were considered moderate and three which were considered low.*
        i. *Is the scope to test all findings that were remediated or just a select few based on criticality and risk? About five of the findings will not be applicable. Of the 14 remaining, we would be open to risk assessing to determine which to test.*
    b. Does SDCERS anticipate sample-based testing of any daily controls that were either enhanced or implemented to mitigate the findings from 2017 Security Risk Assessment report? *No, we don't anticipate there being any frequently occurring (e.g. daily) controls requiring testing.*
        i. *If yes, does SDCERS have a sampling methodology or guidance that they can share for the audit? In the event a daily controls requires testing, Internal Audit's policy is to sample 25.*

23. Of the 19 recommendations from the 2017 Risk Assessment, please provide details of Critical, High, medium and Low risks/findings. *See answer to Question #22 above.*

PRIVACY AUDIT RELATED QUESTIONS

24. Data Privacy Review:
    a. Which privacy regulations and standards are to be leveraged for this review? *This audit is to be evaluated under the AICPA trust framework.*
    b. How many departments are in scope for the audit? *There are approximately seven departments within SDCERS that would be in the scope of the audit.*
    c. Does SDCERS have a data map in place that shows the data flow between different departments and systems? *Not yet, a data map may be compiled after the data inventory is completed, no later than June 30, 2020.*
    d. Does SDCERS have a data inventory of all personal identifiable information (PII) that currently exists in their environment either in physical or electronic format? *SDCERS is currently conducting a data inventory of all PII; this inventory is partially complete and is anticipated to be completed no later than June 30, 2020. The data is saved in an electronic format.*
    e. How many systems, including applications and databases/data warehouses/data stores, are in scope for the data privacy review? *SDCERS utilized just under ten applications and databases/data warehouses/data stores.*

25. The Data Privacy Review does not mention the new California Consumer Privacy Act (CCPA). Is a separate audit plan anticipated to evaluate SDCER's privacy program for compliance with the CCPA? Or might this audit plan be revised in the future to include a compliance review with CCPA? *SDCERS is not subject to the CCPA. Accordingly, an audit plan is not required to address the CCPA.*

26. Has SDCERS implemented FIPPs or GAPP? Briefly describe the existing privacy structure at SDCERS. *SDCERS' Privacy Program framework is based upon the standards in FIPPs. The Privacy Program is relatively new and is currently in a repeatable maturity level pursuant to the AICPA/CICA privacy maturity model.*

27. Do you want to use the GAPP PMM for scoring or an alternative scale? *The scoring set forth under AICPA Trust Fiduciaries should be utilized.*

BCP AUDIT RELATED QUESTIONS

28. Is a defined BCP with periodic audits in place? Has SDCERS conformed to ISO 22301 or has it been certified? *There is a defined BCP; however, the program has not been independently audited or opined on. SDCERS' does not benchmark to ISO and has not been formally certified by a 3rd party.*

GENERAL QUESTIONS

29. Is the requirement of 15 million in errors and omissions insurance something SDCERS would be willing to consider lowering/negotiate on? *Yes, this can be negotiated.*

30. We carry $10 million in errors and omission insurance coverage, not $15 million. Can we obtain a waiver for this? *The requirement of 15 million in errors and omissions insurance may be negotiated, at SDCERS' discretion, after we receive written responses to the RFP.*

31. Will our company be required to have $15M at time of proposal submission or at time of contract award? *See answer to Question #29; this can be negotiated.*

32. How were the hours estimated on page 5 for the different audits? Are these hours estimated based on historical reference? *Hours represent our best guess based on SDCERS' size, the audit's nature, and typical hours needed for internal audits.*

33. On page 4, a footnote indicates that "For the FY2020 IT Audit Plan, the Chief Internal Auditor allocated a total of 110 hours to assist in the IT audit, 70 hours for the IT General Controls Audit and 40 hours for the Internal and External Network Penetration Testing. Assistance includes but is not limited to project management, testing or reporting"; however, on page 5 the table shows the level of effort for ITGC as 250 hours and Internal and External Pen testing as 120 hours. What is the correct number of hours for both ITGC and Internal and External Pen testing? *The ITGC hours of 250 are the hours the external vendor is anticipated to need for the audit. The Chief Internal Auditor budgeted an additional 70 hours of her time, mainly to help with project management and likely reporting, which brings the total budgeted hours to 320. The Internal and External Network Penetration Testing hours of 120 are the hours the external vendor is anticipated to need for the audit. The Chief*

Internal Auditor budgeted an additional 40 hours of her time, mainly to help with project management and likely reporting, which brings the total budgeted hours to 160.

34. Regarding the requirements related to 'Knowledge transfer to the SDCERS Internal Audit department'. The foot note mentions 'Assistance includes but is not limited to project management, testing or reporting'. Please elaborate the timelines (during performance/ post-performance, whether it is testing effectiveness of controls, reporting to whom?) *Hours represent our best guess based on the audit's nature and typical hours needed for internal audits. A more fine-tuned budget will not be available until the specific audit is planned; however, we anticipate:*
    - *About eight hours on project kick-off/planning for both the ITGC and penetration testing audits*
    - *About three hours per week on project managing (e.g. status update meetings, questions, workpaper review, etc.), so about 24 and 18 hours for the ITGC and penetration testing audits, respectively*
    - *About 20 hours on testing for the ITGC audit*
    - *About 18 hours and 14 hours on drafting and finalizing the internal audit report for the ITGC and penetration testing audits, respectively. The internal audit reports are customized and issued by the Internal Audit Department to the Audit Committee/Board of Trustees. For examples of SDCERS' internal audit reports, please see this link https://www.sdcers.org/About-SDCERS/Internal-Audit-Reports/Current-Year.aspx.*

    The hours itemized above are in addition to the hours of 250 for the ITGC and 120 for the penetration testing included in Attachment A of the RFP.

35. Will prior audit lead sheets, workpapers, and reports be available when performing the work? *Internal Audit will provide you with any/all workpapers considered useful. However, most workpapers and reports are not IT in nature, but more finance and operations focused. We have standardized workpapers for Planning, Fieldwork and Reporting that you can tailor for the audit(s).*

36. Can we look at the previous assessments? *Yes. In addition, see answer to Question #35 above.*

37. Can we see criteria for RISK in the Past? *Yes. In addition, see answer to Question #35 above.*

38. Do the audits need to be performed on site, or can some of this work be done remotely? *Yes, some of the work can be performed remotely; however, we anticipate planning the audits (including interviews) to be performed on site.*

39. How much of SDCER's IT environment is outsourced to service providers? *SDCERS out sources application support, voice and data network support, server, desktop Active Directory and email support.*

40. Is there an approved or target budget for the entire audit or for any individual audit? *Authority was delegated by SDCERS' Board to staff to spend up to $100,000 per year over the next three years on the five IT-related audits.*

41. For the risk control matrix, which control framework is most appropriate (e.g. NIST Cyber Security Framework or its overlay with NIST SP 800-53)? *With each internal audit, a risk control matrix is created and tailored to the audit. NIST SP 800-53 is the most appropriate starting point, but only the risks and controls associated with the objective(s) of the audit would be included on the audit-specific risk control matrix.* Is the intended assessment planned to be based on rev4 or rev 5 (in final draft as of writing) of SP 800-53? *Assessment should be based on the most current literature (so rev 5 if available at the time of the audit).*

42. What is the RISK control matrix you want us to utilize? *See answer to Question #41 above.*

43. Has SDCERS gained any ISO related certifications, such as ISO 27001? *SDCERS' does not benchmark to ISO and has not been formally certified by a 3rd party.*

44. Do you have a formal Risk Eval process? *SDCERS' performs an annual risk assessment for all areas of SDCERS (e.g. IT, Benefits Administration, HR, etc.) and uses this risk assessment to develop the Internal Audit Plan. The last IT-specific Risk Assessment was completed in 2017.*

45. Any other Frameworks? NIST, AICPA? *No, not at this time.*

46. Can additional work be proposed? *Yes, we are open to additional suggestions.*

47. GAPS in general audit? *SDCERS received an unqualified opinion on our FY18 CAFR. See link herein:* https://www.sdcers.org/Investments/Annual-Reports/Current-Year/SDCERS-FY-2018-CAFR.aspx

48. Any additional regulatory bodies or laws? *No.*