Request for Quote – Security Auditor and Related Services Q&A

- Assess
    - Network vulnerability
        - Can you provide an indicative scope of testing i.e., number of systems/ IP addresses / Subnets to be assessed?

          Network mapping
          Service Evaluation
          Unauthenticated vulnerability scanning
          Authenticated vulnerability scanning

        - Is both internal and external network assessments considered in-scope?
          Yes – IP range will be provided.

    - Application vulnerability
        - Can you provide an indicative scope of testing i.e., number of applications (web, thick client, mobile apps, etc.) to be assessed?
          30 internal web applications.

          What is the size of the in-scope applications to be assessed [small (<=10 dynamic pages), medium (<30 dynamic pages, Large (>30 dynamic pages)]
          Medium
        - Are there only external facing applications or internal applications as well in scope of assessment?
          Internal only

    - Application code review
        - Can you provide an indicative scope of assessment i.e., number of applications, lines of code, custom applications/software products, etc.?

          Lines of code: C# 100,000; HTML 50,000; JavaScript: 30,000; CSS 10,000
        - Does NCEL have the tools and infrastructure for source code scanning? Is there specific tool (e.g., fortify, AppScan, etc.) that is preferred to be used?
        - Will NCEL provide remote access to enable access to the code scanning solution/infrastructure or does it have to be performed on-site only? on-site only

    - Wireless security
        - How many physical locations and access points are in scope of assessment (e.g., location, buildings, floors, no. of access points, etc.)?

1 building; 2 floors; 40 AP’s

- Is the scope to perform a guided discovery and assessment or a penetration attempt/un-announced war-driving?

- Security policy and processes / privacy program management / Security organization and governance
  - How many physical locations and access points are in scope of assessment (e.g., location, buildings, floors, no. of access points, etc.)? Headquarters, 1 building, 2 floors, 6 entries and warehouse. Five total regional office.
  - Is there a list of laws, regulations, and industry standards that NCEL is required to meet? Please identify the ones that it already meets vs. any that it plans to meet.
    - We follow both ISO and NIST standards along with Industry Standards MUSL rule 2.
  - Please confirm if NCEL has identified a list of security controls that can be used for security and compliance purposes or is the objective to derive or enhance the control set as part of the engagement. Yes
  - Please confirm if NCEL has a security governance structure in place. Yes

- Technology infrastructure and security controls
  - Can you provide an indicative scope of technology infrastructure to consider in scope of this assessment E.g., server, routers, databases, firewalls, middleware, etc.? Yes
  - Does NCEL have documented and maintained network architecture or defense architecture that provides defense in depth? Yes
  - Does NCEL have documented hardening standards followed for its technology infrastructure components? Yes

- Regional Office Security, Warehouse Security
  - Number of physical locations for which physical security evaluation has to be performed? Two locations out of the five regional offices
  - What is the rough estimate of the employees having access? 20 to each locations
  - What is the access management system implemented (e.g. card based, PIN, Biometrics, etc.)? card access

- Assess Disaster Recovery/Business Continuity Planning
  - Please confirm if NCEL has an existing BCP and DRP in place which is current? Yes, the most recent is from 2016. We have not had a chance to update it to reflect the recent building move.

  - Please confirm if NCEL performs regular testing of its BCP and DRP including failover tests to see if Austin site picks up the load in case of primary failure? So, for the CGS related fail overs, yes. I we do that semiannually. For the most part, Joe Norman's group handles that. For the business side of the house, we typically perform table top exercises but we have not in some time. That is a task that Tim Rink has to have one conducted. However, we have had a lot of issues for resources due to the conversion, the building move, Keno and other projects.]
  - Please confirm if the test results are documented and are available for analysis? They should be. As I said, Joe Norman's group maintains the process for the fail over.

- Review systems, connections and administrative policies and procedures that permit access to and monitoring of all NCEL locations

  - Are the systems that support the access to NCEL locations part of other technical assessment such as network VA, technical infrastructure assessment, etc.? Yes

- Assess security of NCEL's second chance drawings and RNG machines

  - Since second change drawings are submitted through web application, are the web applications in scope for assessment? If you are asking if I would like to have it be part of the scope, I would like it to be.]
  - What are the Backend systems of second change drawings? Are they considered in scope as part of network VAPT (penetration testing)? Again, if you are asking if I would like to have it be part of the scope, I would like it to be.
  - Is the assessment scope to be one-time for this year or multiple periodic assessments? Assessment scope if includes 2016-2017
  - Is there a specific deadline to complete all assessment and provide our reports/recommendation? Would like to present the final report to our Audit Committee during the March 6th commission meeting.
  - Will NCEL permit execution of feasible assessment activities remotely from offshore locations? No

- **Page 9, Item a) Assessment scope**

  - Could you please outline the scope of the network vulnerability assessment?
    Network mapping
    Service Evaluation
    Unauthenticated vulnerability scanning
    Authenticated vulnerability scanning
  - Could you please provide a list of the applications or the number for the application vulnerability assessment?
    40

- Could you please indicate the approximate number of lines of code for the application code review?
  C# 100,000
  HTML 50,000
  JavaScript 30,000
  CSS 10,000
- Page 9, could you please define/describe “freeware tools”.
  N/A
- Will the system provider have resources and information available to complete the assessment?
  N/A

- **Page 10, item i, Do you have any specific IT Audit training requirements?**

  Training that can help improve our IT internal audit skills for normal internal audit duties. For example we currently preform continuous monitoring audits that include reviews of active network user ids, SDLC, change management, Data and System file backups, anti-virus scan reviews, etc. Just looking for training that can help improve our audit techniques and skills.
  Page 10, item j, Can you please clarify and/or confirm the need to provide audit working papers in addition to the final report deliverable?
  Past security auditors have given us the option of retaining working papers to review the results of testing. It helps to prevent any audit overlap or gaps in testing between external auditors and internal auditors.

Thanks,

Best Regards,

Anthony Downey
Purchasing Administrator