Central Bank of The Bahamas Response to Vendor Questions

Re: ISU20211004 - Acquisition and Implementation of a Next Generation Security Incident and Event Monitoring Solution

---

Question: Can you please provide a list of the organizational and regulatory compliance frameworks that CBOB must comply with?

Answer: There are no mandated cybersecurity frameworks. However, the Bank does reference the following frameworks NIST, CIS, OWASP, and ISO 270001 in establishing its security baseline.

Question: What criteria will CBOB be using in its selection of the final deployment model?

Answer: The Bank is seeking a solution that is sufficiently robust in its ability to both adapt and scale to meet the Bank's evolving needs.

Question: Is CBOB most interested in an on-premise or cloud-hosted solution?

Answer: See above response.

Question: For file integrity monitoring, please provide quantity of Windows, Linux and OS/400 devices to be included in the scope of the engagement?

Answer: Presently, the Bank will require FIM services for approximately one hundred windows based systems, approximately thirty Linux servers and two AS/400 LPAR's.

Question: Please specify any specific log data storage retention requirements?

Answer: At minimum, the solution should accommodate 1 year cold log storage and 3 months hot log storage.

Question: For each of the TWO sites in scope, please provide a breakdown of the following:

Answer: Note approximations in table below. Specific details regarding technologies in production use will be shared during a detailed scoping exercise following vendor selection and contract award.

	Production	DR	VPN Tunnels
Number of users	>300	>300	>10
Please describe your network in detail including the type of connectivity between sites, i.e. VPN, hub and spoke, distributed via MPLS, etc. i. Internet bandwidth ii. Any High Availability implementations	i.Between sites we have 500 Mbps production and DR facilities, VPN connection bandwidth ii.Yes, there is high availability at both MPLS and DIA circuits.		>15
Number of Firewalls	4	4	>15
Number of Switches	>30	>10	N/A
Number of Routers	N/A	N/A	N/A
Remote access Architecture and Technologies (VPN, Citrix, Netscaler)	Yes, a mixture of VPN & Virtual Desktop.		N/A
Number of servers	>300	>200	N/A
How many of these would you consider mission critical (RTO of 8hrs or less)	>100	>50	N/A
Number of Workstations	>350	N/A	N/A
Number of VDI hosts	>10	N/A	N/A

Question: Please describe your current endpoint protection solution(s) including any Endpoint Detection and Response (EDR) technology and the number of endpoints covered?

Answer: The Bank leverages an on-premise agent based endpoint protection solution. Specific details regarding technologies in production use will be shared during a detailed scoping exercise following vendor selection and contract award.

Question: Please describe your vulnerability management program including scanning platform(s) in use, frequency of scans, and approximate number of devices scanned per occurrence?

Answer: The Bank leverages an industry leading vulnerability scanner for vulnerability detection. Scans are performed daily, weekly and on an ad-hoc basis against approximately 800 assets.

Question: Please describe your usage of DLP or File Integrity Monitoring?

Answer: N/A

Question: Please describe any web content filtration and/or proxy technology currently in place. (E.g. Umbrella, Zscaler)?

Answer: The Bank currently deploys an industry leading web content filtering solution. Specific details regarding technologies in production use will be shared during a detailed scoping exercise following vendor selection and contract award.

Question: Network Access Control (NAC)?

Answer: Yes, specific details regarding technologies in production use will be shared during a detailed scoping exercise following vendor selection and contract award.

Question: Third-party threat intelligence sources?

Answer: N/A

Question: Privileged Access Management?

Answer: N/A

Question: Cloud Access Security Broker (CASB)?

Answer: N/A

Question: How much hot (searchable immediately) and cold (searchable in a certain amount of time) log storage is needed monthly/annually?

Answer: At minimum, the solution should accommodate 1 year cold log storage and 3 months hot log storage.

Question: Are any of the sites directly connected to the Internet or do they come back through corporate or a data center to access the Internet?

Answer: Both sites are directly connected to the internet. Specific configuration details will be provided during the scoping exercise following vendor selection and contract award.

Question: If Direct Internet Access (DIA) is enabled to any sites, describe the technical architecture supporting that (e.g. split tunnel VPN) and the number of sites configured with DIA

Answer: The Bank has two sites provisioned with DIA circuits. Specific configuration details will be provided during the scoping exercise following vendor selection and contract award.

Question: Please describe your Active Directory architecture in detail, including:

a. **the number of forests**
b. **the number of domains**
c. **the number of domain controllers, and each component's location.**
d. **Do you utilize Active Directory-integrated DNS and DHCP?**

Answer:

a. 1
b. 1
c. 4 DCs
d. Yes

Question: Do you utilize a premises-based or cloud-based email platform?

Answer: Hybrid

Question: Please describe in detail including platform, licensed users, license type, email gateway/spam filtration in use.

Answer: The Bank has a layered email gateway security architecture with a hybrid modelling. The solution is spec-ed to accommodate the current user base. More specific details will be provided during the scoping exercise following vendor selection and contract award.

Question: Please describe your usage of any Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) cloud implementations, including platform(s) in use, number of VPC/VNET, container environments, virtual machine instances, and cloud storage repositories.

Answer: N/A

Question: Please describe any other critical security or technology components of your environment not covered above.

Answer: N/A

Question: Please provide details surrounding cloud-based services and log sources currently in use that will be included in the scope of the solution.

Answer: The Bank uses various SaaS deployments to support specific operational functions. Specific details will be provided during the scoping exercise following vendor selection and contract award.

Question: How many assets you wanted to be analyzed by the full packet capture solution?

Answer: Approximately 150 assets

Question: What's the utilized bandwidth to be monitored by the Full Packet Solution?

Answer: 1 GB

Question: AS/400 Amount of LPARs that needs to be monitored?

Answer: Four (4)

Question: Given that this proposal is due right after Thanksgiving, we are asking if the dates can be pushed by 1 week.

Answer: Due to pre-existing timelines, the Bank is unable to offer any extension to the stated deadline.