AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

# INITIAL RISK ASSESSMENT QUESTIONAIRE FOR THE ENTERPRISE

## Inventory and control of Enterprise Assets Questions:

**I)** Does THE ENTERPRISE have a record and/or process to maintain an accurate, detailed, and up to date inventory of all enterprise assets that process or store data including end-user devices(laptop/mobile), network/security devices, non-computing/IOT devices and servers? This includes physically, virtually, and remotely.

**II)** Is there a record and/or process to maintain an accurate, detailed, and up-to-date inventory of assets that are regularly connected to the enterprise infrastructure even if they are not under the control of THE ENTERPRISE?

**III)** Is there a process that exists to remove unauthorized assets on a weekly/biweekly basis?

**IV)** Is there an active discovery tool to identify THE ENTERPRISE assets connected to the network?

**V)** Does DHCP logging exist on all DHCP servers or IP address management tool to update the enterprise asset inventory?

**VI)** Does THE ENTERPRISE use a passive discovery tool to identify assets connected to the network?

**VII)** Does THE ENTERPRISE utilize port level access control. 802.1X to control which device can authenticate to the network?

**VIII)** Is client certificate tied to the 802.1X authentication to authenticate hardware assets connecting to the trusted network?

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Inventory and control of Software Assets Questions:

**I)** Is there a list or process to maintain a detailed software inventory of all licensed software installed on THE ENTERPRISE's assets? This should include: title, publisher, deployment mechanism, business purpose, initial install date, version, app store(s)/Uniform Resource Locator (URL)

**II)** Is there a risk acceptance policy with sufficient mitigating controls for unsupported software to run on THE ENTERPRISE's assets that is necessary for the fulfillment of THE ENTERPRISE's mission?

**III)** Is there a process to block/remove unauthorized software without exception or expired exception monthly?

**IV)** Is there a software inventory tool to help THE ENTERPRISE automate the discovery and documentation of installed software?

**V)** Does THE ENTERPRISE use technical controls such as application whitelisting to ensure only authorized software can execute or be accessed?

**VI)** Does THE ENTERPRISE use technical controls to ensure only authorized libraries such as .dll, .ocx, .so…files are allowed to load into a system process?

**VII)** Does THE ENTERPRISE use technical controls such as digital signatures and version control, to ensure only authorized scripts such as .ps1, .py, etc files are allowed to execute?

**VIII)** Is there a process for physically/logically segmenting systems used to run required business software but incurs higher risk for THE ENTERPRISE?

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

**Continuous Vulnerability Management Questions:**

**I)** Is there a vulnerability management program that utilizes compliant scanning tools to automatically scan all systems on the network weekly for potential vulnerabilities?

**II)** Are systems equipped with agents to perform authenticated vulnerability scans locally or remote scanners configured with elevated rights to perform this task?

**III)** If a VM scanner exist, is there a dedicated service account for authenticated vulnerability scans, tied to a specific machine and IP address and should not be used for other administrative activities?

**IV)** Is there an automated software update tool in place to ensure operating systems are running the most recent security updates provided by the software vendor?

**V)** Is there an automated software update tool in place to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor?

**VI)** Are results from consecutive vulnerability scans compared to verify vulnerabilities have been remediated in a timely manner?

**VII)** Is there a risk-rating score process to prioritize the remediation of discovered vulnerabilities? E.g. From Critical priority to Low priority

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Inventory of Administrative Accounts Questions:

**I)** What process or automated tool exist to record all administrative accounts including domain and local accounts to ensure that only authorized individuals have elevated privileges?

**II)** Is there a process that exist before deploying of any new asset to change the default passwords for consistent values with administrative level accounts?

**III)** Is there a process that exist to ensure all users with administrative account access use a dedicated account for elevated activities? This account should only be used for admin activities and internet browsing, email, or similar activities.

**IV)** Is there a process to ensure that when multi-factor authentication is not supported (e.g. Service Accounts), accounts will use complex passwords that are unique to that system and saved in a secure password manager with 2FA/Multifactor authentication enabled?

**V)** Is multifactor authentication technology and encrypted channels for all administrative account access whether on-site or through a third-party provider currently in use?

**VI)** Is there a dedicated machine for administrators to use for administrative task access? Typically, it should be segmented from the primary network without internet access. It should also not be used for reading emails, composing documents or similar activities.

**VII)** Is there a procedure/process to limit access to scripting tools (Microsoft PowerShell and Python) to only administrative/development users with the need to access those capabilities?

**VIII)** Are the systems configured to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges?

**IX)** Are systems configured to issue a log entry and alert on unsuccessful logins to an administrative account?

+234 807 238 9851 aif secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Secure Configuration for Assets and Software on Assets Questions:

**I)** Is there a well-maintained security configuration standard for all authorized operating systems and software with a process to update them regularly?

**II)** Is there a secure image/template for all systems with approved configuration standards? Usually, any new system deployment or existing system that becomes compromised should be imaged using one of those templates.

**III)** Are the master images and templates on a secured server and validated with integrity monitoring tools to ensure only authorized changes to the images are possible.

**IV)** Does a system configuration management tool exist to automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals?

**V)** Is there a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements and alerts when unauthorized changes occur?

**VI)** Is there any technology to facilitate assets and environment micro and macro segmentation?

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Monitoring, and Audit Log Analysis Questions:

**I)** Are there at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in the logs are consistent?

**II)** Has local logging been enabled on all systems and networking devices for correlation, analysis, and alert on a log analytics platform?

**III)** Is the system logging enabled to include detailed information such as event source, date, user, timestamp, source address, destination address and other useful metadata?

**IV)** Is there an established process to maintain the collection, review, and retention of audit logs for THE ENTERPRISE's assets? If yes does the document get reviewed and updated on a recurring basis?

**V)** Does THE ENTERPRISE collect DNS and URL request query logs of all assets?

**VI)** Are the systems that store logs secure and have adequate storage space for the logs generated?

**VII)** Are the appropriate logs being aggregated to a central log management system for analysis and review?

**VIII)** Is there a Security Information and Event Management (SIEM) or log analytic tool (XDR) for log correlation and analysis?

**IX)** Are logs being reviewed on a regular basis to identify anomalies and abnormal events?

**X)** If a SIEM exist, is it regularly tuned to better identify actionable events and decrease event noise?

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

## Monitoring, and Audit Log Analysis Questions Continued:

**XI)** Does THE ENTERPRISE collect command-line audit logs from Powershell, BASH and remote administrative terminals?

**XII)** Does THE ENTERPRISE retain logs for a minimum of 90days?

**XIII)** Does THE ENTERPRISE collect logs where applicable of service providers connecting to its network? Including authentication and authorization events, data creation, user management and disposal events

**XIV)** Does THE ENTERPRISE have an inventory of all service provider that connects to the network through a secured connection

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Data Protection Questions:

**I)** Does THE ENTERPRISE have a data management process? If yes, does it address data sensitivity, data ownership, handling of data, data retention limit and disposal requirements?

**II)** Is there a data inventory for sensitive data based on the data management process?

**III)** Is there a data access control list/permissions based on users need to know for local and remote file system, database, and applications?

**IV)** Is there a data retention policy according to THE ENTERPRISE's data management process? And does it include minimum and maximum timelines?

**V)** Is there a secure dispose of data according to the data management process? If yes, does it commensurate with data sensitivity?

**VI)** Are the end user devices containing sensitive data encrypted? Using implementations such as Windows BitLocker, Apple FileVault, Linux dm-crypt or other third-party software?

**VII)** Is there a data classification scheme at THE ENTERPRISE? Typical labels include "Sensitive", "Confidential" and "Public."

**VIII)** Is there a documentation of data flow including your service provider data flow based on your data management process?

**IX)** Are all removeable media that can connect to THE ENTERPRISE's assets encrypted?

**X)** Is THE ENTERPRISE's sensitive data in transit using secure protocols like Transport Layer Security (TLS), Datagram Transport Layer Security (DTLS) and Open Secure Shell (OpenSSH)

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

## Data Protection Questions Continued:

**XI)** Are sensitive data at rest on Servers, Applications and Databases encrypted using storage/Server layer encryption or Application/Client-side encryption with additional measures on the storage devices such as “Plain-text data storage not allowed”?

**XII)** Is the network and storage segmented for data processing and storage based on sensitivity of data?

**XIII)** Is there a host-based and network data loss prevention tool to identify all sensitive data stored, processed, or transmitted through THE ENTERPRISE’s assets? Including those located onsite or at remote locations.

**XIV)** Does THE ENTERPRISE log sensitive data access including modification and disposal?

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Account Management Questions:

**I)** Is there a process established to maintain an inventory of all accounts managed by THE ENTERPRISE? This must include both user and administrative accounts. I should contain the person's name, username, start/stop dates, and department. Also are all active accounts validated on a recurring schedule.

**II)** Are all THE ENTERPRISE's assets configured to used unique passwords? 8-Character password for accounts using MFA and a 14-Character password for accounts not using MFA.

**III)** Is there a process to Delete or Disable any dormant accounts after a period of 45 days of inactivity?

IV) Is there a process to establish and maintain an inventory of service accounts, validate they are active and authorized on a recurring schedule? The inventory at a minimum must contain department owner, review date and purpose.

V) Does THE ENTERPRISE centralize account management through a directory or identity service?

+234 807 238 9851 aif secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Account Control Management Questions:

**I)** Is there an established process (Preferably automated) for granting access to enterprise assets upon new hire, rights grant, or role change of a user?

**II)** Is there an established process (Preferably automated) for revoking access to enterprise assets through disabling accounts immediately upon termination, rights revocation or role change of the user. Disabling accounts instead of deleting accounts may be necessary to preserve audit trails.

**III)** Does THE ENTERPRISE require all externally exposed assets or third-party applications to enforce MFA. When supported MFA through a directory service or SSO is a cleaner safeguard?

**IV)** Is MFA required for remote network access into THE ENTERPRISE's corporate network

**V)** Is there a process to maintain, review and update the inventory of the enterprise authentication and authorization systems including those hosted on-site or at the remote service provider?

**VI)** Does THE ENTERPRISE centralize access control for enterprise assets and applications through a directory service, Identity provider or SSO provider where supported?

**VII)** Are role-based access control (RBAC) defined and maintained through determining and documenting access rights necessary for each role to successfully carry out its assigned duties?

**VIII)** If **VII** is yes, does THE ENTERPRISE perform Access Control reviews of assets and validate on a recurring schedule that all privileges are authorized?

+234 807 238 9851 aif secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

**Email and Web Browser Questions:**

**I)** Does THE ENTERPRISE asset configuration ensure only fully supported browsers and email clients provided through the vendor are allowed to execute?

**II)** Does THE ENTERPRISE use a DNS filtering service on all enterprise to block access to unapproved and malicious domains?

**III)** Does THE ENTERPRISE enforce and update network-based URL filters across onsite, virtual, and remote assets to prevent assets from connecting to potential malicious or unapproved domains/websites?

**IV)** Does THE ENTERPRISE enforce browser and email client security through restricting, uninstalling, or disabling any authorized or unnecessary extensions and add-on application?

**V)** Does THE ENTERPRISE implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting with implementing the Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) standard?

**VI)** Is THE ENTERPRISE security policy configured to block unnecessary file types attempting to enter the email gateway?

**VII)** Does THE ENTERPRISE have an email security protection product that includes anti-malware attachment scanning and/or sandboxing etc.?

+234 807 238 9851 aif secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Malware Defense Questions:

**I)** Does THE ENTERPRISE have deployed on all assets anti-malware software?

**II)** Are automatic updates for anti-malware signatures configured for all THE ENTERPRISE's assets?

**III)** Are auto-run, auto-play and auto-execute functionality disabled for removable media?

**IV)** Is the anti-malware software configured to automatically scan removable media?

**V)** Are anti-exploit features enabled on THE ENTERPRISE's assets and software such as Microsoft Data Execution Prevention (DEP), Windows Defender Exploit Guard (WDEG), Apple System Integrity Protection (SIP) and Gatekeeper?

**VI)** Is the anti-malware software behavior based and centrally managed?

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

**Data Recovery Questions:**

**I)** Does THE ENTERPRISE have and maintain a data recovery process to address recovery activities, recovery prioritization and the security of the backup data? If yes, is it reviewed and updated annually or when significant changes occur?

**II)** Does automated backups of in-scope assets occur weekly, bi-weekly, or more frequently based on the sensitivity of data?

**III)** Is the recovery data protected with equivalent controls as the original data? Refer to ***DATA PROTECTION QUESTIONS***

**IV)** Is there an established and maintained isolated instance of recovery data with implementations to include version control, and backup destinations through offline, cloud and off-site systems or services?

**V)** Is the backup recovery tested quarterly or more frequently by sampling in scope THE ENTERPRISE's assets?

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Network Infrastructure Questions:

**I)** Is there a process to ensure the network infrastructure is kept up to date by running stable release of the software and/or using Network-as-a-service (NAAS)? With a review monthly or more frequently.

**II)** Is there a process to establish and maintain a secure network architecture. A secure network architecture must address segmentation (Macro & Micro), least privilege, confidentiality, and availability at a minimum.

**III)** Does THE ENTERPRISE securely manage its network infrastructure using version-controlled Infrastructure-as-code and use of secure network protocols like SSH and HTTPS with adequate encryption strength?

**IV)** Is there a network architecture diagram and other network system documentation, with a process to review and update annually or when a significant change occurs?

**V)** Is the Network AAA server centralized with limited authentication attempts if any?

**VI)** Does THE ENTERPRISE use secure network management (SNMPv3) and communication protocols (802.1X, Secure File Transfer Protocol, WI-FI Protected Access 2(WPA2) Enterprise, WPA3 or greater)

**VII)** Does THE ENTERPRISE require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on the end-user device?

**VIII)** Does THE ENTERPRISE have and maintain dedicated computing resource (Physically and logically separated without access to the internet and segmented from THE ENTERPRISE's primary network) for all administrative task or tasks requiring administrative access with an acceptable timeout period?

**IX)** Is there a process to change the default passwords for devices and removal of unnecessary accounts?

**X)** Is TCP keep-alive enabled along with disabling outbound management connections from a device?

**XI)** Is route authentication for dynamic routing protocols enabled while disabling default vlan?

+234 807 238 9851 aif secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Network Monitoring and Defense Questions:

**I)** Does THE ENTERPRISE have a Host-Based and Network/Cloud Service Provider Intrusion Detection and Prevention system that is properly tuned?

**II)** Is traffic filtering and similar network system grouping between network segments in THE ENTERPRISE's environment performed where appropriate?

**III)** Is the physical connection between the border router connected to the ISP and edge firewall well configured? i.e. ensure the border router is not connected to the internal or management subnets.

**IV)** Does THE ENTERPRISE IT team stay updated with vendor-supported hardware?

**V)** Does THE ENTERPRISE enforce compliance and access control to enterprise network/resource? based on "Up to date anti-malware software installed, software patch update etc. To ensure complaint assets are on the network.

**VI)** Does THE ENTERPRISE collect network traffic flow logs from network devices to review and alert on suspicious/malicious connections?

**VII)** Is port level access control utilizing 802.1X or similar network access control protocol like certificates used for user and/device authentication.

**VIII)** Does THE ENTERPRISE employ application layer filtering implementation such as filtering proxy, application layer firewall/gateway?

**IX)** Is there a process to tune security events alerts thresholds monthly or more frequently?

**X)** Is IP source routing disabled and Unicast reverse-path forwarding enabled on external interfaces?

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

## Network Monitoring and Defense Questions continued:

**XI)** Are unused interfaces disabled and interfaces port properly connected?

**XII)** Are unnecessary dynamic trunking disabled along with enabling port security?

**XIII)** Are port mirroring and proxy Address Resolution Protocol (ARP) disabled?

**XIV)** Did THE ENTERPRISE put up notification and consent banners in devices to provide notice to users that connecting to the device is for "authorized use only" and the system is subject to monitoring?

**XV)** How does THE ENTERPRISE facilitate the secure connectivity of remote users into the network and connect the HQ to other branch sites securely?

+234 807 238 9851 aif secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Security Awareness and Skills Training Questions:

**I)** Is there an established and maintained security awareness program? With training at hire and at a minimum annually?

**II)** Are the workforce members trained to recognize social engineering attacks such as phishing, pre-texting, and tailgating?

**III)** Are the workforce members trained on the benefits of MFA, Password Complexity and Credential Management?

**IV)** Are the workforce members trained to identify, properly store, transfer, archive and destroy sensitive data? Including locking their screen when they step away, erasing physical and virtual whiteboards at the end of meetings and storing data and assets securely?

**V)** Are the workforce members aware of the causes for unintentional data exposure? e.g. mis-delivery of sensitive data, publishing data to unintended audiences, leakage of company secret/source codes, losing portable end-user devices, reputation destruction.

**VI)** Are the workforce members able to recognize a potential incident and report it to the right personal/team?

**VII)** Are the workforce members trained to verify and report out-of-date software patches or any failure in automated process or tools to the IT personnel/team?

**VIII)** Are the workforce members trained on the dangers of connecting to and transmitting data over insecure networks for enterprise activities?

**IX)** Is role-specific security awareness and skills training conducted for IT/Security professionals (OWASP top 10 vulnerability awareness and prevention training for web application developers) and Advanced social engineering awareness training for high-profile roles?

+234 807 238 9851 aif secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Service Provider Management Questions:

**I)** Does THE ENTERPRISE have and maintain an inventory of service providers with classification(s) with an employee contact for each service provider? If yes, is the document reviewed and updated annually or when significant change occurs.

**II)** Is there an established and maintained service provider management policy which address the classification, inventory, assessment, monitoring and decommissioning of service providers?

**III)** Are the service providers classified with one or more characteristics such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk and mitigated risk with update and review annually or when significant changes occur?

**IV)** Does the service provider contracts include security requirements such as security incident and/or data breach notification and response, data encryption requirements and data disposal commitments. It should be consistent with the service provider management policy and the security section should be reviewed annually.

**V)** Is there a process to access service providers and may include review of standardized assessment reports such as Service Organization Control 2 (SOC 2), Payment Card Industry (PCI), Attestation of compliance (AoC), customized questionnaires or appropriate rigorous process?

**VI)** Is there a process to monitor THE ENTERPRISE's service providers compliance, release notes, publications, and dark web according to the service provider management policy?

**VII)** Is there a way to securely decommission service providers? Which include user and service account deactivation, termination of data flows and secure disposal of enterprise data within the service provider systems.

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Application Software Security Questions:

**I)** Is there an established process to maintain a secure application development process? The process should include secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code and application security testing. The document should be reviewed and updated annually or when a significant change occurs.

**II)** Is there an established process to address reports of software vulnerabilities, including providing a means for external entities to report? Third-party application developers need to consider this an externally facing policy to set expectations for outside stakeholders.

**III)** Is there a vulnerability handling policy that identifies reporting process, responsible party for handling reports and a process for intake, assignment, remediation, and remediation testing?

**IV)** Is root cause analysis performed on security vulnerabilities? to allow development teams move beyond just fixing individual vulnerabilities as they arise?

**V)** Is there an established and updated inventory of third-party components used in development? Often referred to as "Bill of Materials", the inventory includes any risks that each third-party component could pose.

**VI)** Is there a process to utilize trusted third-party software components as well as established and proven frameworks and libraries that provide adequate security?

**VII)** Is there a process to establish and maintain a severity rating system for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed? This process should include setting a minimum level of security acceptability for releasing code or applications.

**VIII)** Are the industry recommended hardening configuration templates for application infrastructure components been used. Includes the underlying servers, databases, webservers, cloud containers, Platform as a Service (PaaS) components and Software as a Service (SaaS) components. Allowing in-house developed software to weaken hardened configuration should not be allowed.

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

## Application Software Security Questions continued:

**IX)** Does THE ENTERPRISE have separate environments for application production and non-production (Development and Testing) systems?

**X)** Is there a process to ensure all software development personnel receive training in writing secure code for their specific development environment and responsibilities? Training should be annually and design a way to promote security within development team.

**XI)** Does THE ENTERPRISE apply secure design principles in application architectures? This includes the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input", turning off unprotected ports and services, renaming/removing default account, removing unnecessary programs and files etc.

**XII)** Does THE ENTERPRISE leverage vetted modules/services for application security components such as identity management, encryption, auditing, and logging to reduce developer's workload and minimize the likelihood of design or implementation errors?

**XIII)** Does THE ENTERPRISE use only standardized, currently accepted, and extensively reviewed encryption algorithms?

**XIV)** Does THE ENTERPRISE apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed?

**XV)** Is authenticated and unauthenticated penetration testing being performed for critical applications to find business logic vulnerabilities?

**XVI)** Is threat modelling being conducted to identify application security design flaws within a design before code is created? It is conducted by specially trained individuals who evaluate the application design, architecture, and infrastructure in a structured way to understand its weakness and gauge security risks for each entry point and access level.

+234 807 238 9851 aif secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Incident Response Management Questions:

**I)** Is there at least one key person and one backup to manage THE ENTERPRISE's incident handling process? Management personnel are responsible for the coordination and documentation of incident response and recovery efforts but can consist of third-party vendors or a hybrid approach.

**II)** Is there an established process to contact parties that need to be informed of a security incident. This can include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners or other stakeholders. Verification should be done annually to ensure information is up to date.

**III)** Is there an established process for the workforce to report security incidents? It should include timeframe, personnel to report to, mechanism for reporting and the minimum information to e reported while ensuring this process is publicly available to all workforces.

**IV)** Is there an established incident response standard that addresses roles and responsibilities, compliance requirements and a communication plan annually or when significant changes occur?

**V)** Are key roles and responsibilities for incident response assigned including staff from legal, IT, information security, facilities, public relations, human resources, incident responders and analysts as applicable.

**VI)** Is there a process to determine which primary and secondary mechanisms will be used to communicate and report during a security incident? Mechanisms can include phone calls, emails (This can be affected during an incident) or letters and review annually or when a significant change occur.

**VII)** Is there a plan to conduct routine incident response exercises/scenarios for key personnels involved in the incident response process to prepare for responding to real-world incidents? This should test communication channels, decision making and workflow on a annual basis at a minimum.

**VIII)** Is there a process to conduct post-incident reviews to help prevent incident recurrences through identifying lessons learned and follow-up action.

**IX)** Is there a process to maintain security incident thresholds, differentiating between an incident and an event e.g. abnormal activity, security vulnerability, security weakness, data breach, privacy incident etc. Kindly review annually or when significant changes occur.

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

**Business Continuity Questions:**

**I)** How does THE ENTERPRISE deal with deliberate threats? This includes Labor strike/protest, physical vandalism/attack, Theft of critical assets, cyber-attack such as ransomware, malware.

**II)** How does THE ENTERPRISE deal with accidental threats? This includes fire/explosion, equipment/hardware malfunction, power failure, chemical/hazard spill, software malfunction, supplier failure/bankruptcy, industrial accidents

**III)** How does THE ENTERPRISE deal with natural hazards? Epidemic/pandemic, earthquake, hurricane, heatwave, snowstorm, flooding/tidal wave, extreme heat/cold temperatures.

**IV)** How does THE ENTERPRISE deal with generic threats and lockdowns? Illness in the community, key players and managers absent, space availability, fuel disruption, electricity disruption, communication disruption, transportation infrastructure.

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Penetration Testing Questions:

**I)** Is there an established and maintained penetration testing program appropriate for the size, complexity, and maturity of THE ENTERPRISE? The scope should include network, web application, Application Programming Interface (API), hosted services and physical premise control.

**II)** Is there a process to plan the engagement rules and findings of the penetration testing program such as excluded attack type, acceptable hours, frequency, limitations, and retrospective requirements

**III)** Is there a process to perform external penetration testing no less than annually? It would include the enterprise and environmental reconnaissance to detect exploitable information, can be white or black box testing and must be conducted through a qualified party as it requires skills and experience.

**IV)** Is there a process to remediate penetration testing findings based on THE ENTERPRISE's policy for remediation, scope, and prioritization.

**V)** Is there a process to validate the defensive security measures after each penetration test? E.g. modify rules and capabilities to detect techniques and/or addition of more defensive technologies.

**VI)** Is there a process to perform internal penetration testing based on the program requirements, no less than annually? It can be white or black box testing.

+234 807 238 9851 aif secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Cyber Threat Intelligence Questions:

**I)** Does THE ENTERPRISE have an established and well-maintained and documented CTI program that is well-designed with repeatable processes and effective use of relevant technologies to ingest the intel?

**II)** Does THE ENTERPRISE have an established and well-maintained governance structure to oversee, coordinate and receive cyber threat function?

**III)** Is there a periodic review for each intelligence sources to measure their effectiveness, relevancy, credibility, and the ability to provide value? E.g. of threat intel platforms include. Cisco Talos, FBI InfraGard, ThreatCloudAI by checkpoint, OpenCTI, AutoFocus by Palo-alto, Trusted Automated Exchange of Indicator Information (OpenTAXII), Microsoft Defender Threat Intelligence, Google Mandiant Threat Intelligence etc.

**IV)** Is the sharing of intelligence to internal and external sources/third parties been reviewed for legal and regulatory compliance?

**V)** What role does the CTI function perform to THE ENTERPRISE. Feed security tools with current data to prevent cyber-attacks? support operational security requirements (Red teaming, playbook dev or threat hunting), ensure critical vulnerabilities are identified and addressed? Support the adoption of a strategic view of the threat landscape? Or all the above.

**VI)** Does THE ENTERPRISE have a process to monitor and address all the information shared publicly by employees and it's supply chain organizations?

**VII)** Are the Sources and Agencies (SANDAS) mapped to Intelligence requirement (IR) and priority intelligence requirements (PIR)?

**VIII)** Does the CTI program produce internal intelligence report, threat modelling, Indicators of Compromise (IOC), Threat Assessments, Significant Acts Reporting (SIGACTs), Intelligence Summaries (INTSUMs), Thematic reporting, attack scenarios for testing with the red team? This should be shared with the CISO and board.

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

## Cyber Threat Intelligence Questions continued:

**IX)** Is there a process to feed back intelligence improvements/failures identified through real-life incidents back to the intelligence cycle?

**X)** Are the operation hours of intelligence equal to that of the wider detection, protection, and response team?

**XI)** Is machine learning and Artificial intelligence performed on basic and/or advanced intelligence analysis?

**XII)** Is the element of creating threat models, SIGACTS or Threat Alert automated where possible?

**XIII)** Do all the intelligence feed sources go into a centralized location or dispersed across various security solutions?

**XIV)** Does the program collect and ingest both structured and unstructured data into standardized format?

**XV)** Do the intelligence sources include both internal (Human, CCTV, Logs) and external (Industry insiders, dark net forums, YouTube, streaming channels, social media, OSINT sources, industry peers, Technology intelligence, Governments/arm's length Government sources, Geopolitical sources, Regulatory and compliance sources) resources?

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Cyber Threat Hunting Questions:

**I)** Does THE ENTERPRISE have an established, well-maintained, process oriented and documented Threat-hunting capability?

**II)** Where does the Threat hunting team collect key security data points from in the IT/Security infrastructure?

**III)** How does THE ENTERPRISE detect adversary Tactics Techniques and procedures (TTP's) and other Indicators of Compromise (IOC) during a threat hunt? This can be through campaign tracking and active sharing of IOCs e.g. domains, URLs, and hashes.

**IV)** How does the threat hunting team create, develop, and test new hypothesis? E.g. through review of threat intelligence, automated cyber risk scoring (Crown Jewel analysis), alerts backtracking, attacker's mindset/TTP.

**V)** What tools does the threat hunting team use for testing hypothesis? These include SIEM or log analysis tools, visualization and graph searches, automation of threat hunting procedures.

**VI)** Is the threat hunting capability integrated with the tools, and automated procedures with analytics to continuously improve alerting capabilities with machine learning.

+234 807 238 9851 aif_secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Identity Access Management and Privilege Access Management Questions

**I)** Does THE ENTERPRISE have an established, well-maintained, and documented IAM and PAM program?

**II)** Does THE ENTERPRISE enforce multifactor authentication, single sign-on and biometric authentication for all onsite users, remote users, and assets?

**III)** Does THE ENTERPRISE have a centralized identity store/directory service with a process for reviewing role-based, administrative, and privileged users?

**IV)** Is the IAM policy if any integrated with machine learning/artificial intelligence and predictive analytics such as User and Entity Behavior Analytics tools (UEBA) to identify and mitigate threats in real time?

**V)** Is there a process for provisioning and deprovisioning (preferably automated) role- based access to apps, mobile apps, and infrastructure?

**VI)** Is there a process for provisioning and deprovisioning (preferably automated) administrative and privileged users when they terminate?

**VII)** Is there a process for eliminating shared administrative account, and maintaining an immutable audit trail for privileged accounts e.g. shared accounts, and service accounts?

**VIII)** Does THE ENTERPRISE have a complex password policy, session management, control, auditing, alerting, and recording for any privileged account? This should be integrated with SIEM/XDR

**IX)** Is there an accurate inventory of administrative local accounts, privileged accounts, and passwords?

**X)** Is there a password/ssh key vault with automatic periodic rotation for all administrative accounts?

**+234 807 238 9851** **aif_secure@protonmail.com** **13 Olufunmilola Okikiolu Street Ikeja, Lagos.**

AIF TECHNOLOGY SERVICES

AKINKUNMI OLA
CEO/CTO

## Identity Access Management and Privilege Access Management Questions continued

**XI)** Is there an integration with IT service management (ITSM) to drive access control request to service help desk?

**XII)** Do all administrators have least privilege access on login with elevation policies such as just-in-time or just-enough privileges?

**XIII)** Is there a process to eliminate hardcoded credentials and config data from applications, scripts, and local account via identity consolidation for Unix and Linux?

**XIV)** Is there a policy to prevent privileged access by client system that isn't known, authenticated, properly secured and trusted?

**XV)** Is there a policy for privileged access control management for vendors and contractors connecting to THE ENTERPRISE's applications and systems?

**XVI)** Is there a process to automate privileged security in Devops workflow and tooling?

**XVII)** Are privileged identities limited to the applications and systems that they require immediately through time-bound and temporary privilege access?

**XVIII)** Does a process exist to automatically detect and respond to anomalous privilege activity?

**+234 807 238 9851** **aif_secure@protonmail.com** **13 Olufunmilola Okikiolu Street Ikeja, Lagos.**

**REFERENCES:**

I) https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf
II) https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF
III) https://www.infragard.org/
IV) https://workbench.cisecurity.org/benchmarks/547
V) https://www.england.nhs.uk/wp-content/uploads/2023/04/part-1-d-business-continuity-plan-template.pdf
VI) https://halifaxpartnership.com/sites/default/uploads/How-We-Help-Section/3.-BCM-Toolkit-Guide-Risk-Assessment.pdf
VII) https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
VIII) https://workbench.cisecurity.org/communities/132
IX) business continuity risk assessment template university of Strathclyde Scotland
X) https://www.threathunting.net/files/framework-for-threat-hunting-whitepaper.pdf
XI) https://globalitresearch.com/wp-content/uploads/2023/10/delinea-whitepaper-pam-maturity-model.pdf
XII) https://www.crest-approved.org/buying-building-cyber-services/cyber-threat-intelligence-maturity-assessment-tools/
XIII) https://optimalidm.com/iam-maturity-assessment/
XIV) https://www.beyondtrust.com/blog/entry/shared-accounts-for-it-administration-how-to-maximize-the-benefits-minimize-the-risks
XV) https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf