

John Uwahamen Usiabulu

Leicester, Leicestershire Le1 6ff | 07459031405 | uwajohn101@outlook.com

Career Summary

Detailed-oriented Information Security Analyst with over five years of hands-on experience ensuring the assurance and adherence of security practices aligned with organization policies, regulatory requirements, and applicable laws. Experience in Information Technology Security, Information System Auditing, and Information Assurance with a focus on Internal Controls, auditing, risk assessments, audit engagements, and developing security policies, procedures, and guidelines. I am a highly skilled and enthusiastic Desktop engineer/ Project Coordinator with excellent stakeholder management, communication, and inter-personal skills. I have the relevant skills to prioritize deliverables, influence and motivate others. Able to manage stakeholder expectations and willing to take full responsibility for project management office functions. I enjoy challenging and diverse roles and I am confident working individually or as part of a team.

Profile

-
- Active Directory and group policy management, user security and access management, roles and privileges, files sharing, remote desktop support, O365 administration, and computer hardware management (repairs and maintenance)
 - Azure active directory (create or edit users, assign administrative roles to others, reset user passwords, manage user licenses, and manage domains).
 - Systems/Network security management (WAN/LAN), End point and gateway security management (deploying updates and security policies)
 - Server virtualization/migration, Windows/Mac operating systems troubleshooting/support, Windows desktop, unified communications, and cloud setup. Experienced with SCCM, JAMF, and other desktop management tools.
 - Proven experience as a Systems Administrator, Network Administrator and Desktop Support Engineer providing 2nd and 3rd line support.
 - Software integration and deployment and application support.
 - General ICT Troubleshooting and problem-solving skills.
 - Excellent communication skills.
 - I am a Cisco certified expert.
 - Certified Cisco Cybersecurity Essentials.
 - Strong Customer Service and Communication skills.
 - Utilized internal ticketing and case management tool for all incidents, changes made, communication with end users and possible escalations to second level support.
 - Experienced in Virtualization of servers, VMWare and Vsphere whereby the new vSphere tools and REST APIs increase consolidation, flexibility, and automation for easy configuration access and maintenance. "With the application-focused management and simplified lifecycle which can increase agility and our pace of innovation."

- I have a good understanding of designing and implementing new network solutions which are Scalability and modularity, Performance, Availability and reliability and Security and Cost.
- Expertise in Digital Forensics and Penetration testing.
- Skilled in IP, UDP , TCP, Gn /S5/S8, Radius, DIAMETER (including Gx , Gy and Sy protocols).

Skills

-
- Regulatory Compliance Audit & Reporting
 - Customer trust and Third-party due diligence
 - Third-Party & Vendor Security Assessments
 - Customer Security Communication & Reporting
 - Risk Management & Mitigation
 - Security Assurance Frameworks & Best Practice
 - Security Policy & Compliance Audits
 - Security Policy & Procedure Development Contractual
 - Security Agreement Review
 - Security Frameworks (e.g., ISO 27001, NIST, PCI DSS)
 - Security Awareness & Training
 - Security Control Implementation & Monitoring

Experience

Centre for policy and development advocacy

Information Security Analyst. Nottingham UK

10/2022 – Till Date (Part-Time)

Responsibilities:

- Facilitate and successfully lead regulatory audits, ensuring compliance with industry standards and regulations.
- Spearhead efforts in preparing teams for external and internal audits, coordinating resources, and ensuring a smooth audit process.
- Liaise with external auditors, addressing queries and providing required documentation promptly.
- Orchestrate comprehensive pre-audit reviews, aligning IT, business, and security operations to regulatory standards.
- Review and respond to audit findings, ensuring timely remediation and implementing preventive measures for the future.
- Present post-audit findings to executive leadership, recommending strategic changes and securing buy-in for security improvements.
- Collaborate with internal departments to identify, mitigate, and report on potential compliance vulnerabilities.

- Conduct in-depth security assessments of third parties, ensuring they meet our security standards before engaging in business partnerships.
- Review security documentation received from vendors, highlighting potential areas of concern.
- Evaluate vendor security protocols, practices, and documentation, ensuring they align with our internal security standards and best practices.
- Evaluate the security posture of third parties, such as partners or service providers, to ensure their practices align with organizational security standards.
- Engage with vendors to guide them through the security assessment process, provide feedback on findings, and recommended mitigation strategies.
- Maintain the third-party and vendor security database, ensuring all evaluation records are up to date.
- Review and provide input on contractual agreements to ensure they include necessary security clauses, responsibilities, and liabilities.
- Provide customers with security documentation and complete detailed questionnaires to ensure they have full visibility into our security practices.
- Establish a trust framework ensuring customers have confidence in our security posture, including periodic communication and transparency initiatives.
- Lead customer security assurance initiatives, ensuring customers have confidence in our security posture through periodic reviews, detailed documentation, and direct communications.
- Continuously address customer security queries, ensuring rapid responses and resolutions.
- Collaborate with the legal and compliance teams to ensure alignment of security practices with data protection regulations, such as GDPR, ISO, PCI and CCPA.
- Collaborate with the customer support team to address and escalate security-related inquiries, ensuring timely resolution.
- Present risk metrics and reports to senior leadership, ensuring visibility and understanding of the current risk posture.
- Maintain a comprehensive risk register, tracking all identified risks, associated controls, and mitigation status.
- Collaborate closely with the IT and operations teams to integrate risk management practices into the development and deployment of new systems and applications.

Tizeti

Network Administrator, Lagos Nigeria

08/2019 – 09/ 2021

- Provided desktop support and troubleshooting for over 100 users in a fast-paced group wide corporate environment.
- Managed and maintained Active Directory, Group Policy, and SCCM
- Implemented and maintained software and security updates on all desktop computers.
- Assisted in the deployment of new hardware and software to users.
- Resolved tickets in a timely manner using a ticketing system.
- Compiled project status report on a weekly basis from order managers and workstream lead.

- Organized and facilitated issue resolution meetings responsible and provided general support services to IT Managers.
- I was a key member of the Project team for the successful delivery of the migration program. I was engaged through the project lifecycle, from inception to completion.
- Provided support and guidance to Project Managers and Business Analyst.
- I promoted appropriate communication and reporting to ensure alignment, mitigation management and progress across teams and stakeholders.
- Used Project planning tools in the management of milestones, risk management, outlined deliverables, activities, resources, schedules, milestones, communications.
- Collated MI packs and reports; and send to the finance and order management team.
- Collated project issue log and maintained record of issues for each project. Documented the benefits and risks associated with a project.
- Tracked resources, costs, time sheets, project status (RAG) and reports on order spreadsheet.
- Schedule Work stream weekly meeting - complete minutes/actions, Risks, and Issues Log.
- Managed detailed scheduling, tracking, and reporting of various stages of release cycles.
- Ensured all pre-requisites are covered and completed from governance processes.

EDUCATION:

De Montfort University, UK.
BSc Cybersecurity.

Auchi Polytechnic Auchi, Nigeria.
HND Polymer Technology.

PROFESSIONAL QUALIFICATIONS/CERTIFICATIONS:

- Certified in Cybersecurity Essentials.
- Information Technology Infrastructure Library ITIL
- Comptia S+
- CCNA.

References available on request.