**Temi Akindele Kuyoro**

**CISA | CISM | CRISC | CDPSE | AWS | PCI-QSA**

**Houston, TX 77406**

**848-468-0700**

**toppymo@gmail.com**

**Personal Profile**

* Certified IT Risk, Governance, and Compliance (GRC) professional with over 12 years of experience leading cyber security programs, managing regulatory audits, and conducting risk assessments for financial, healthcare, and technology industries.
* Proven expertise in building high-performing teams, implementing security frameworks, and mitigating third-party risks.
* Proficient in PCI DSS, NIST 800-53, ISO 27001, and SOX compliance. Adept at aligning security initiatives with business objectives while fostering collaboration across stakeholders.

**Education**

* UNIVERSITY OF MAINE, ORONO MAINE, M.Sc. Information Systems
* OBAFEMI AWOLOWO UNIVERSITY, ILE-IFE NIGERIA, B.Sc. Management and Accounting

**Professional certifications:**

* Certified Information Systems Auditor (CISA)
* Certified Information Security Manager (CISM)
* Certified Data Privacy Solutions Engineer (CDPSE)
* Certified in Risk and Information Systems Control (CRISC)
* PCI Qualified Security Assessor (PCI-QSA)
* Certified Information System Security Professional (CISSP) In view

**Key skills:**

* Leadership and Team Development
* Risk Management and IT Governance (GRC)
* Regulatory Compliance (SOX, PCI DSS, HIPAA, GDPR, CCPA)
* Cyber security Frameworks (NIST, ISO 27001, HITRUST, COBIT)
* Third-Party/Vendor Risk Assessment
* IT General Controls (ITGC) Auditing
* Device Hardening and Security Control Validation
* Cloud Security (AWS, Azure) and Identity Management
* Security Policy Development and Training
* Audit Coordination and Remediation

**Technical Tools & Platforms**

* Governance Tools: Archer eGRC, Jira, Confluence
* Cloud Platforms: AWS (Landing Zones, IAM), Azure
* Security Tools: TrendMicro, Active Directory, PowerShell
* Productivity: Microsoft Office Suite, Google Workspace

**Core Value:**

* Delivering proactive IT governance and risk management solutions to protect organizational assets, enhance compliance, and align IT practices with business objectives.

**Core Qualifications:**

* Good understanding of security control frameworks: PCI DSS, COSO, COBIT, HITRUST, SOC, NIST 800-53, FISMA and ISO 27001.
* Payment Card Industry Data Security Standard (PCI DSS)
* Information security and computer network access
* Information Technology General Controls Auditing.
* Cloud Control Matrix (CCM),
* Vendor/ Third Party Risk Management
* Cloud Security Assessment
* Federal Financial Institution Examination Council (FFIEC)
* Data Privacy: CCPA, GDPR
* IT Compliance
* Policy Development
* Network Security Systems
* Firewall
* Remediation Management
* Project Management
* Strong communication skills
* Leadership

**Professional Work Experience:**

**WEX INC, South Portland Maine.**

**April 2018 – PRESENT**

**Team Lead, Information Security Compliance**

* Oversee the design and implementation of new systems, ensuring the protection of information and corresponding processes supporting company policies, procedures, and standards.
* Participated with external auditors in the coordination of all regulatory compliance activities e.g., Hitrust, HIPAA, NIST, PCI, SOX, and SOC.
* Participated in the development and oversight of required corrective action plans relating to security compliance and PCI issues.
* Supports line of business PCI self-assessments and third party QSA lead PCI assessments.
* Worked closely with subject matter experts including Risk, Audit, Lines of Business, Legal, Compliance, external and 3rd party vendors to ensure compliance with requirements of PCI DSS, NIST SP 800-53, HIPAA, HITRUST and other relevant security requirement.
* Developed and reviewed security policies, procedures, standards, and guidelines in support of the Information Security and Compliance program.
* Extensive experience ensuring compliance with GDPR, CCPA, HIPAA, or other relevant data protection laws and regulations
* Conducted Data Protection Impact Assessments (DPIAs) to evaluate and mitigate risks in handling personal data.
* Established and maintained a robust data governance framework, ensuring data accuracy, availability, and protection.
* Monitored compliance with IT security policies through regular audits and penetration testing.
* Developed and implemented policies and procedures in alignment with FFIEC IT Examination Handbooks.
* Coordinated with various departments to maintain up-to-date knowledge on regulatory changes and ensured adherence to FFIEC standards.
* Provided training and awareness programs on FFIEC compliance requirements to internal teams.
* Developed compliance training roadmap and strategies for data protection, prevention and 3rd party security risks.
* Performed security audits, risk assessments and impact analysis, identify gaps, and implemented mitigating controls.
* Coordinated, documented, and reported on internal investigations of possible security violations.
* Facilitated and coordinated the enterprise-wide Risk Assessment.
* Worked with external assessors and subject matter experts (SMEs) in the identification and interpretation of the Hitrust CSF requirements.
* Develop and execute Corrective Action Plans (CAPs) to address audit findings and ensure continuous improvement.
* Maintained information security plan and all associated security control documents and ensured systems and networks are following NIST 800-53 and categorization of systems.
* Collaborated with management to maintain fire wall management
* Conducted comprehensive device hardening for servers, endpoints, and mobile devices to ensure compliance with organizational security standards and best practices, including CIS benchmarks.
* Developed and implemented automated scripts and tools to enforce baseline configurations and monitor system hardening status.
* Performed security controls validation through regular vulnerability assessments, penetration tests, and compliance audits, identifying and mitigating risks promptly.
* Identifies Plan of Action Milestone (POA&M) and provides SME recommendations for solutions.
* Facilitates the collection, analysis, and presentation of key security metrics monthly to senior management.
* Led the implementation of the Cloud Control Matrix framework to enhance cloud security posture.
* Conducted gap analyses to identify and address deficiencies in cloud security controls.
* Developed and maintained a detailed inventory of cloud security controls, ensuring alignment with CCM guidelines.
* Implemented continuous monitoring and risk management processes for cloud environments.
* Developed PowerShell scripts in the collection and reporting of monthly metrics dashboard.
* Designed, defined, planned, and evaluated the information security systems and architecture.
* Assisted in evaluating and determining goals for short, medium, and long-term project plans.
* Provided project management skills, including developing project plans, budgets, and deliverables schedules.
* Developed a positive environment, monitoring workloads of team members, while meeting the enterprise goals and respecting work-life quality of team members.
* Leading third party attestations of IT security, including access controls, asset management, network security, incident response, firewall and switch configurations, workstation hardening, etc. for a Fortune 100 technology firm

**Key Achievements:**

* Reduced vendor-related security risks by 25% through enhanced third-party assessment protocols.
* Spearheaded the adoption of automated tools for compliance reporting, improving team efficiency by 30%.
* Introduced a risk-based compliance training program, increasing employee awareness by 40%.

**BDO, New York NY**

**Feb 2016 - Mar 2018**

**Senior Cyber Security Compliance SME**

* Managed cybersecurity projects for clients in financial, healthcare and technology industries.
* Project planning participation with project managers, business analyst and team members to analyze business requirement and outline propose IT solution for clients across various industries.
* Managed cybersecurity projects for clients across various industries.
* Conducted annual security audits- audited control design and control effectiveness for network infrastructure, application security, data loss prevention, anti-malware, incident response and metrics reporting.
* Performed regulatory compliance audits including SOX, PCI, NIST and HIPAA.
* Audit planning, testing, budgeting and reporting.
* Engagement kicking off with all relevant parties, setting timelines and expectations for all major engagement milestones and determining potential audit risks.
* Provided support for IT SOX audits for controls testing relating to access control, change management and IT operations.
* Reported audit findings and advise on remediation efforts.
* Assisted in preparing business application owners prior to external audits.
* Configured multi-account architecture, identity and access management, governance, data security, network design and logging within provisioned AWS Landing Zones.
* Provisioned AWS Landing Zones to create a customized baseline of AWS accounts, networks and security policies.
* Ensured clients environment and patterns meets defined security standards.
* Interviewed, assessed, and documented major financial service vendor compliance with IT risk, security and regulatory requirements and control.
* Designed network and application vulnerability assessment programs and testing methodologies.
* Performed Risk assessment, developed and review system security plans (SSP), Plan of Action and Milestones (POA&M) Security Control Assessment, Configuration Management plan (CMP), Contingency plans (CP), and other tasks and specific security documentation in accordance with NIST SP 800-37 rev 1, 800-18, 800-53 rev 3 and 800- 34.
* Conducted onsite and virtual 3rd party risk assessment based on agreed procedure guidelines.
* Owned responsibility over third -party security vendor assessments to ensure vendors have the level of security to balance the level of risk they introduce to the organization.
* Collaborated with vendors to ensure identified gaps are remediated within agreed on timeframe.
* Conducted IT controls risk assessment including reviewing organizational policies, standards, and procedures and providing advice on their adequacy, accuracy, and compliance with industry standards.
* Prepare Security Assessment and Authorization (SA&A) packages to ascertain that management, operational and technical security controls adhere to NIST SP 800-53 standards.
* Ascertained all FISMA documents are updated within 6months of a new policy release.

**Key Achievements:**

* Improved client audit outcomes by implementing robust remediation strategies for regulatory compliance.
* Mentored junior consultants, increasing team productivity and improving client satisfaction scores.

**TD Bank Consulting, Cherry Hill NJ**

**May 2014 – Jan 2016**

**Senior IT AUDITOR**

* Managed cybersecurity projects for clients in financial, healthcare and technology industries.
* Project planning participation with project managers, business analyst and team members to analyze business requirement and outline propose IT solution for clients across various industries.
* Conducted annual security audits- audited control design and control effectiveness for network infrastructure, application security, data loss prevention, anti-malware, incident response and metrics reporting.
* Performed regulatory compliance audits including SOX, PCI, NIST and HIPAA.
* Audit planning, testing, budgeting, and reporting.
* Engagement kicking off with all relevant parties, setting timelines and expectations for all major engagement milestones and determining potential audit risks.
* Provided support for IT SOX audits controls testing relating to access control, change management and IT operations.
* Reported audit findings and advise on remediation efforts.
* Assisted in preparing business application owners prior to external audits.
* Configured multi-account architecture, identity and access management, governance, data security, network design and logging within provisioned AWS Landing Zones.
* Provisioned AWS Landing Zones to create a customized baseline of AWS accounts, networks, and security policies.
* Ensured clients environment and patterns meets defined security standards.
* Interviewed, assessed, and documented major financial service vendor compliance with IT risk, security and regulatory requirements and control.
* Designed network and application vulnerability assessment programs and testing methodologies.
* Performed Risk assessment, developed and review system security plans (SSP), Plan of Action and Milestones (POA&M) Security Control Assessment, Configuration Management plan (CMP), Contingency plans (CP), and other tasks and specific security documentation in accordance with NIST SP 800-37 rev 1, 800-18, 800-53 rev 3 and 800- 34.
* Conducted onsite and virtual 3rd party risk assessment based on agreed procedure guidelines.
* Owned responsibility over third -party security vendor assessments to ensure vendors have the level of security to balance the level of risk they introduce to the organization.
* Collaborated with vendors to ensure identified gaps are remediated within agreed on timeframe.
* Conducted IT controls risk assessment including reviewing organizational policies, standards, and procedures and providing advice on their adequacy, accuracy, and compliance with industry standards.
* Prepare Security Assessment and Authorization (SA&A) packages to ascertain that management, operational and technical security controls adhere to NIST SP 800-53 standards.
* Managed multiple teams of associate across various audit engagements.

**Key Achievements:**

* Enhanced audit cycle efficiency by 20% through process improvements and automation.
* Reduced IT compliance risks by identifying and addressing key control deficiencies

**Crest Consulting Group (CPA), Rockville, MD.**

**Nov 2012 – Jan 2014**

**IT AUDITOR**

* Conducted IT compliance testing to assess risk, evaluate internal controls, safeguard assets, and analyze controls supporting financial reporting and operating procedures.
* Audit planning, testing, and reporting.
* Evaluated IT Compliance gaps and collaborated with management on remediation.
* Performed audit of IT General Controls such as, Access Control, Change Management, IT Operations, Disaster Recovery and Platform Reviews (Windows and UNIX OS) using applicable frameworks like COSO, COBIT and PCI DSS.
* Planned and managed the ITGC audit functions using best practice audit guidelines in compliance with FFIEC and COBIT
* Served as liaison between team and external auditors (EY, Deloitte, KPMG and PWC) in the participation of external auditing activities.
* Managed IT related aspects of financial statements audits, SOX engagements and Service Organization Control Reports (SOC1 & SOC2).
* Performed MAR testing and assist process owners to perform their own self -testing.