CHARLES MENSAH/GRC ANALYST

Oklahoma | +1 405-259-6231 | mensahchle@gmail.com | LinkedIn

SUMMARY

Governance, Risk, and Compliance (GRC) Analyst with 3+ years of hands-on experience strengthening information security programs, driving risk management efforts, and ensuring alignment with frameworks including NIST 800-53, ISO 27001, HIPAA, SOC 2, and PCI DSS. Proven ability to execute security control assessments, manage third-party/vendor risk, write and maintain critical security documentation, and support both internal and external audit readiness. Skilled in risk evaluation, POA&M management, and continuous monitoring, with a strong track record of collaborating across security, compliance, and IT teams to maintain a defensible security posture.

ACCOMPLISHMENTS & SKILLS

- Developed comprehensive security documentation, including continuity plans, POA&Ms, and risk assessment reports.
- Created security assessment artifacts such as test plans and security assessment reports.
- Conducted vulnerability assessments using tools including Nessus and Web Inspect.
- Collaborated with audit teams to ensure compliance with ISO 27001, HIPAA, SOC 2, and PCI DSS standards.
- Performed in-depth security control reviews for management, operational, technical, and privacy controls.
- Executed continuous monitoring tasks: scan analysis, updating security documentation, security impact analysis, contingency plan testing, and annual assessments.
- Conducted risk assessments in alignment with industry standards.
- Specialized in POA&M management and enterprise risk management.
- Proficient in GRC tools: SharePoint, Archer, ServiceNow, LogicGate, and OneTrust.
- Skilled in Microsoft Project, Office Suite, Outlook, Excel, and Visio.

SKILLS TOOLS

Governance & Compliance: ISO 27001, HIPAA, PCI DSS, SOC 2
Risk & Audit Management: Risk Assessments, POA&M, Audit Support, Security Assessments
Security Documentation: Policies, Procedures, Business Continuity Plans, Risk Reports, Incident Response Plans, Contingency Plans
Tools: Nessus, WebInspect, Archer, ServiceNow, SharePoint, LogicGate, OneTrust
Continuous Monitoring: Security Control Testing, Impact Analysis, Evidence Gathering, Compliance Reporting
Collaboration & Reporting: Technical Writing, Stakeholder Communication, Security Awareness Training
Office & Productivity: MS Project, Excel, Word, Outlook, Visio

PROFESSIONAL EXPERIENCE

INTEGRIS HEALTH **Oklahoma**
GRC Analyst ***Apr 2024 – Present***

- Led risk assessments for 30+ applications and medical devices, ensuring compliance with HIPAA, PCI DSS, and ISO 27001 frameworks.
- Evaluated security controls, coordinated with stakeholders, and generated POA&M reports with actionable remediation steps.
- Developed and maintained incident response plans, business continuity plans, and contingency plans to strengthen security posture.
- Verified control implementation by reviewing evidence, identifying misconfigurations, and escalating findings to system owners.
- Drove audit readiness by managing documentation reviews, evidence collection, and security testing schedules.
- Performed comprehensive control assessments across management, operational, and technical domains, recommending risk mitigations.
- Collaborated with compliance teams to prepare for ISO 27001, HIPAA, and SOC 2 audits, improving evidence traceability.
- Updated risk templates and policy documentation to align with evolving regulatory compliance requirements.

US BANK CORP **Ohio**
GRC Analyst ***May 2022 – Mar 2024***

- Authored and maintained security policies, continuity plans, incident response procedures, and risk assessment reports for 20+ financial systems.
- Executed control assessment activities including planning, documentation, and continuous monitoring.
- Facilitated risk review sessions, closing 40+ POA&Ms and reducing residual risk exposure.
- Created and managed security assessment reports and risk tracking matrices to validate controls and document corrective actions.
- Conducted vendor risk assessments, identifying 20+ control gaps and tracking remediation in LogicGate and Archer.
- Analyzed vulnerability scan results from Nessus and WebInspect, prioritizing remediation efforts with infrastructure teams.
- Delivered security awareness training on phishing prevention, password hygiene, and mobile security, improving compliance metrics by 25%.
- Partnered with audit and legal teams on SOC 2 readiness, ensuring timely and complete evidence submission.

EDUCATION & CERTIFICATIONS

Bachelor of Science in Computer Science **Sept 2016 – July 2020**
University of Akron – Akron, OH,

- CompTIA Security+
- CISSP (In Progress)