Joycelyn Agyemang

07429003787
joycelyn.agyemang@gmail.com

OBJECTIVE

Seeking an IT Security auditor or assessor position in a growing organization.

CONTROLS & FRAMEWORKS

NIST RMF (FISMA), ISO 27001:2013, ISO 27002:2013, SOC 2 (Type II), SIG Questionnaire, Confidentiality, Integrity, Availability, NIST SP 800-53, 800-53A.

SOFTWARE AND PLATFORM

Archer, Hiperos, One Trust, Bit Sight, Security Scorecard, Microsoft Suite, Google Suite.

SUMMARY OF QUALIFICATIONS

I have over 4 years' experience in conducting comprehensive assessments and review of IT security controls for audited applications and information systems. My expertise includes Conducting Third Party Vendor Risk Assessments, NIST Risk Management Framework (RMF), Information Assurance, System Monitoring, Regulatory Compliance and Loss Mitigation. My knowledge of industry standards and ability to meet milestone deadlines make me a valuable addition to any organization focused on staying on top of information security matters.

CERTIFICATIONS

CompTIA Security+ in progress (expected June 2023)

TRAINING

SIG Questionnaire Overview Training, June 2020
ISO 27001:2013, February 2019
Encryption Awareness training, September 2018
Information Systems Security training, December 2017
Certification and Accreditation Document Review training, January 2016
Phishing Awareness Training, August 2015
FISMA Compliance Training, June 2015
Information assurance awareness training March 2014

EXPERIENCE

Vendor Risk Associate (Contractor) December 2022– Present
Amazon

- Performed third party risk assessments and Vendor due diligence of vendors.
- Monitored 3rd party operational risk trends and provided analysis of data and other operational risk metrics using Security Scorecard.
- Tracked exceptions to IT policies and procedures and followed up with management approval for implementation.
- Used GRC tool, Archer, to conduct application assessment and track issues identified during the assessment with supporting mitigations measures.
- Performed IT & Risk Security Risk & Control Assessments for new products/initiatives.
- Reviewed services provided by vendor and defined scope of assessment.
- Reviewed assessments performed by 3rd party and provided feedback. Defined appropriate risk levels and corrective actions for issues identified.
- Presented issues to 3rd parties and obtained corrective action plans.
- Update procedure documentation to incorporate process changes to SOPs.

Information Security Assessor (Contractor) January 2022– November 2022

Sage Group

- Perform assessments of IS/IT security controls implemented by Rent a Center's external service providers.
- Conduct phone interviews with service providers to clarify processes, understand all technology involved in service delivery and identify control gaps. Conduct follow-up phone interviews with suppliers to validate their response to the remote assessment.
- Identify and assess IT related risks and control weaknesses and coordinate with Rent a Center's Information Security team to define appropriate remediation.
- Collate conclusions and recommendations. Present assessment findings to management regarding the effectiveness and efficiency of control mechanisms.
- Manage scheduling and execution of assessment, document findings and recommendations and provide periodic updates to management.

ISO27001 Compliance Associate (Contactor) May 2020 – January 2022

Pacific Cyber Solutions

- Review ISO27001:2013 and ISO 27002:2013 standards to identify potential gaps in required documentation and processes.
- Assist with creation of Asset register and conduct a test for its relevance.
- Assist in document gathering and evidence collection for audit purposes.
- Document security gaps identified as findings that require remediation and/continuous monitoring.
- Control documents for easy tracking and accountability. Create standard templates for recording data.
- Conduct Risk Assessment and Business Impact Analysis to identify risks that need to be remediated or continuously monitored. Conduct mock audits for various departments.

Cybersecurity Analyst (Contractor) October 2019– January 2020

DHL

- Conduct third-party cybersecurity risk assessments, applying established criteria; Information gathering, questionnaire administration, receive vendor response, risk assessment, reporting and monitoring – using Archer and Bit Sight.
- Support assessment team with quality assurance reviews over work product and reporting.
- Collaborate with internal partners and third parties to mitigate and otherwise resolve third-party cyber risks.
- Consistently deliver on commitments, deadlines and objectives while remaining in scope and leveraging appropriate tools, methods, frameworks, and professional standards.
- Demonstrate consistent credibility with business partners and leadership while recommending initiatives, identifying gaps and potential issues.
- Work independently while representing the services of the department with the highest level of professionalism.
- Appropriately influence business decisions, and the professional judgment for selecting the appropriate methods and techniques to do so.
- Update procedure documentation to incorporate process changes.

IT Risk Auditor (Contractor) December 2017 – July 2019

AstraZeneca

- Determined the scope for system audit. Usually started with a kickoff meeting with key officials and the audit committee.
- Created a test plan to determine controls to be tested as well as methods of testing. Effectively participated in testing of the IT General Controls.
- Conducted audit within specific timeframe utilizing subject matter expects and other system owners Supported requirements gathering and design efforts of critical projects as needed.
- Collected evidence from various point of contacts to update audit finding report for security compliance.
- Tested for effectiveness and adequacy of controls by analyzing test plan against evidence collected via examination, interview and testing.
- Conducted IT controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with company policy.

REFERENCES

References will be furnished upon request.