TOYEEB ATANDA

GRC ANALYST | THIRD-PARTY RISK & AUDIT | SOC 2 | ISRM | CGE-P / CGE-AUD | ISO 27001/27701/42001 LEAD AUDITOR

Augusta, Georgia | atandatoyeeb@gmail.com | linkedin.com/in/toyeeb-atanda | github.com/Toyeeb29 | toyeebatanda.com

PROFESSIONAL SUMMARY

GRC and compliance professional with 4+ years of experience supporting third-party risk management, security questionnaires, SOC 2 audits, internal security risk management, and compliance programs. Experienced coordinating audit engagements end to end, including evidence collection, control mapping, stakeholder interviews, auditor communication, remediation tracking, and audit readiness. Administers GRC and compliance automation platforms for evidence collection, control mapping, risk tracking, and control effectiveness monitoring, with hands-on experience across SOC 2, ISO/IEC 27001, NIST CSF, NIST SP 800-53, HIPAA, and CMMC. Develops security policies, standards, procedures, and runbooks and translates technical security and compliance requirements into clear guidance for business stakeholders, IT teams, executives, and external parties.

CORE COMPETENCIES

Third-Party / Vendor Risk Management (TPRM) · Vendor Security Assessments · Security Questionnaire Response · SOC 2 Audit Support · Evidence Collection · Control Mapping · Risk Register & ISRM · Policy, Standard & Procedure Development · Runbooks · Internal Audit · Gap Assessment · Remediation Coordination · Executive Risk Reporting · Stakeholder Interviewing · Control Effectiveness Monitoring · Audit Readiness Tracking · GRC & Compliance Automation Platforms

Frameworks: NIST CSF · NIST SP 800-53 · NIST SP 800-171 · ISO/IEC 27001 · ISO/IEC 27701 · ISO/IEC 42001 · SOC 2 · HIPAA · PCI DSS · CMMC · GDPR · EU AI Act · NIST AI RMF

PROFESSIONAL EXPERIENCE

HISPI — Project Cerebellum | Adoption & Partnership Co-Lead, United States **2024 – Current**

Promoted twice: AI Adoption Specialist → AI Adoption Working Group Lead → Co-Lead

- **Conducted** AI governance and risk-framework gap assessments for 5+ client organizations against NIST AI RMF and ISO/IEC 42001, coordinating stakeholder interviews to gather control evidence and delivering prioritized remediation recommendations.
- **Led** a 5-person working group driving Trusted AI Model framework adoption to a 50–70% rate, measured by monthly TAIMScore downloads and assessor workshop registration.
- **Drafted and presented** governance risk briefings and framework proposals to executive stakeholders across 5+ organizations, translating technical control requirements for non-technical business audiences.

RapidPaw Cyber Defense | Cybersecurity GRC Consultant (Consulting Engagement), United States **Jul 2024 – Oct 2024**

- **Administered** GRC and compliance automation platforms (Eramba, CSET) for evidence collection, control mapping, and audit readiness tracking, improving operational efficiency by 35%.
- **Led** a 5-person team performing ISO/IEC 27001 and CMMC gap assessments for 3 SME clients, improving compliance readiness 70% and delivering remediation plans to client leadership.
- **Developed** GRC playbooks, procedures, and runbooks standardizing governance and assessment workflows, reducing issue resolution time 20%.
- **Implemented** 15+ custom compliance monitoring rules across EDR, SIEM, and IAM systems to monitor control effectiveness, improving detection accuracy 40%.

Cyber Defense and Intelligence Center (CDIC) | GRC Specialist (Contract), United States **Mar 2024 – Jun 2024**

- **Developed and maintained** security documentation, policies, standards, procedures, and runbooks, establishing the GRC operating charter and governance cadence for an 8-person team.
- **Conducted** third-party security and framework gap assessments (CMMC, ISO/IEC 27001, NIST CSF) across 6+ organizations, documenting 50+ control gaps and advising business and IT owners on remediation.
- **Led** a CMMC Level 1 gap assessment for a startup client, evaluating security practices against the applicable CMMC Level 1 requirements, identifying control gaps, and producing a prioritized remediation roadmap.
- **Identified and prioritized** vulnerabilities using Action1, coordinating remediation across 70+ endpoints, helping technical teams reduce outstanding critical/high-risk findings by 30%+.
- **Designed and delivered** cybersecurity awareness training to 50+ personnel, achieving 95%+ completion across assigned participants.

Genpact | Regulatory & Content Compliance Analyst, Poland **Jul 2022 – Apr 2024**

- **Coordinated** 9 internal and external audit engagements end to end, managing evidence requests, auditor communication, and remediation of identified gaps, sustaining a 90%+ compliance rate.
- **Performed** evidence collection and control mapping across 50+ audit artifacts, interviewing internal stakeholders across 8+ business and operational teams and helping reduce recurring audit findings by 20%.

- **Supported** an information security risk management (ISRM) program aligned to NIST CSF, maintaining the risk register through prioritization, risk acceptance, ownership assignment, and remediation tracking, reducing risk exposure by 50%.
- **Managed** 20+ inbound client, regulatory, and security questionnaire requests per quarter, coordinating evidence from 6+ internal teams and delivering 95%+ of responses on or ahead of deadline.

KEY PROJECTS

HIPAA-Compliant Healthcare API Governance Pipeline **github.com/Toyeeb29/cgep-app-starter**

- Hardened a patient-intake API to HIPAA Security Rule standards with a Terraform baseline (customer-managed KMS keys, S3 Object Lock evidence vault, multi-region CloudTrail).
- Built 6 OPA/Rego policies with automated tests, a signed CI/CD evidence pipeline, and an OSCAL control-to-code mapping; identified and remediated a live credential-exposure finding including key rotation.

ARGUS — AI Governance Compliance-as-Code Engine **github.com/Toyeeb29/argus-ai-grc**

- Engineered a CI-gated pipeline classifying AI systems under the EU AI Act against a control catalog crosswalked to NIST AI RMF and ISO/IEC 42001, generating sealed evidence packs and blocking deployment on critical governance failures.

NISTBOT — Agentic RAG Agent for Control Framework Lookups **github.com/Toyeeb29/nistbot**

- Built a retrieval pipeline (n8n, OpenAI, Pinecone) answering NIST SP 800-53 questions from grounded source passages, replacing manual control-catalog searches with verifiable answers.

CERTIFICATIONS

- Certified GRC Engineer — Practitioner (CGE-P) | Certified GRC Engineer — Auditor Specialty (CGE-AUD)
- ISO/IEC 27001:2022 Lead Auditor — Information Security Management
- ISO/IEC 27701:2025 Lead Auditor — Privacy Information Management
- ISO/IEC 42001:2023 Lead Auditor — AI Management Systems
- CompTIA Security+ ce | ServiceNow Certified System Administrator | Securiti AI Security & Governance
- Microsoft Certified: Security, Compliance & Identity Fundamentals; Azure Fundamentals; Azure AI Fundamentals; Azure Data Fundamentals

TECHNICAL SKILLS

GRC & Compliance Platforms: Eramba, CSET, ServiceNow, n8n

Cloud: AWS (S3, KMS, CloudTrail, Security Hub, IAM), GCP (Workload Identity Federation, Org Policy, Audit Logs), Azure (Entra ID, Azure Policy, Key Vault)

Policy & Evidence Automation: Terraform, OPA/Rego, Conftest, tfsec, GitHub Actions, Cosign keyless signing, S3 Object Lock

Machine-Readable Compliance: OSCAL, compliance-trestle

Languages: Python (boto3), HCL, Bash

LEADERSHIP

Vice President | GRC Engineering Club — Augusta Chapter **2026 – Current**

- Co-founded the Augusta chapter to build a regional community for engineers, auditors, and compliance professionals across the CSRA.
- Connect GRC and compliance practitioners rotating through Fort Gordon's Army Cyber Command, the Signal Corps, and the Georgia Cyber Innovation & Training Center.

Global Ambassador | Global Council for Responsible AI — USA Chapter **Oct 2025 – Current**

- Champion public awareness and education on responsible AI, activating local and digital communities to expand engagement and impact.

EDUCATION

MSc, Environmental Protection and Management — Jagiellonian University, Kraków, Poland