

TOYEEB ATANDA

GRC ENGINEER | SECURITY & PRIVACY | ISO 27001/27701/42001 LEAD AUDITOR | CGE-P / CGE-AUD

Augusta, Georgia | atandatoyeeb@gmail.com | [linkedin.com/in/toyeeb-atanda](https://www.linkedin.com/in/toyeeb-atanda) | github.com/Toyeeb29

PROFESSIONAL SUMMARY

GRC Engineer with 4+ years of experience designing and automating governance, risk, compliance, and privacy programs for cloud-native environments. Experienced building continuous compliance pipelines using Terraform, OPA/Rego, GitHub Actions, and AWS services to automate evidence collection, verify security controls, and improve audit readiness across SOC 2, ISO/IEC 27001, ISO/IEC 27701, HIPAA, NIST SP 800-53, and AI governance frameworks. Passionate about applying AI to reduce manual GRC work while strengthening security assurance, enabling engineering teams, and improving measurable risk outcomes.

PROFESSIONAL EXPERIENCE

Adoption and Partnership Co-Lead | HISPI — Project Cerebellum

2024 – Current

Previously: AI Adoption Working Group Lead; AI Adoption Specialist

- Champion adoption and partnership strategy for the Trusted AI Model (TAIM) framework, guiding 5+ organizations through AI governance and risk-framework integration aligned to NIST AI RMF and ISO/IEC 42001
- Lead a team of 5, driving an adoption rate of 50–70%, measured by TAIMScore monthly downloads and stakeholder attendance and registration at the TAIMScore Assessor Workshop
- Advanced from AI Adoption Specialist to Working Group Lead to Co-Lead, assuming expanded scope after the Partnership and Adoption working groups merged
- Partner with cross-functional stakeholders across adoption and partnership functions to advance responsible AI adoption within client organizations

Regulatory and Content Compliance Analyst | Genpact, Poland

Jul 2022 – Apr 2024

- Led cross-functional teams through 9 internal and external compliance audits, achieving a 90%+ compliance rate
- Evaluated 50+ pieces of audit evidence, mapping technical controls to audit requirements and reducing audit findings by 20%
- Supported development of a risk management and regulatory oversight program aligned to the NIST framework, reducing risk exposure by 50%

GRC Specialist | Cyber Defense and Intelligence Center, United States

Mar 2024 – Jun 2024

- Established the GRC operating charter for a team of 8, defining governance processes and operating cadence
- Conducted risk assessments and gap assessments against multiple frameworks and standards across client organizations
- Identified and prioritized vulnerabilities using Action1 and related tooling, coordinating remediation with technical teams
- Designed and delivered cybersecurity training programs to strengthen organizational security awareness

KEY PROJECTS

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 and evaluating a control catalog crosswalked across EU AI Act, NIST AI RMF, and ISO/IEC 42001
- Automated generation of SHA-256-sealed evidence packs and model cards, blocking deployment on critical governance failures

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

- Built an agentic retrieval pipeline (n8n, OpenAI, Pinecone) that answers questions about NIST SP 800-53 by retrieving grounded passages instead of guessing, replacing manual control-catalog searches with instant, verifiable answers

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

- Hardened a healthcare patient-intake API to HIPAA Security Rule standards using 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 and secure repository remediation

Multi-Cloud Compliance Automation Lab (github.com/Toyeeb29/cgep-labs)

- Built compliant-by-default Terraform modules and keyless OIDC/Workload Identity Federation CI/CD authentication across AWS and GCP, with OSCAL control documentation

Real-Time AI Incident Logging (No-Code) (medium.com/@atandatoyeeb)

- Built a no-code Zapier pipeline ingesting AI Incident Database RSS feeds, classifying severity via AI, and delivering real-time Slack alerts and a Google Sheets risk register

AI Readiness Tracker with Airtable (medium.com/@atandatoyeeb)

- Designed an Airtable-based AI governance tracker with linked AI inventory, risk register, and controls tables, featuring a compliance dashboard and automated alerts for non-compliant or critical-risk systems

LEADERSHIP

Vice President | GRC Engineering Club — Augusta Chapter

2026 – Current

- Co-founded the Augusta to build a regional community for engineers, auditors, and compliance professionals across the CSRA
- Connecting 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

CERTIFICATIONS

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

TECHNICAL SKILLS

- **Cloud:** AWS (S3, KMS, CloudTrail, Security Hub, IAM), GCP (Workload Identity Federation, Org Policy, Audit Logs), Azure (Entra ID, Azure Policy, Key Vault)
- **IaC & Policy as Code:** Terraform, OPA/Rego, Conftest, tfsec
- **CI/CD & Evidence:** GitHub Actions, CircleCI, Cosign keyless signing, S3 Object Lock
- **Machine-Readable Compliance:** OSCAL, compliance-trestle
- **Frameworks:** NIST 800-53, HIPAA Security Rule, SOC 2, PCI DSS, EU AI Act, NIST AI RMF, ISO/IEC 42001/27001/27701
- **Languages:** Python (boto3), HCL, Bash

EDUCATION

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