

TOYEEB ATANDA

GRC ENGINEER & AUDITOR | COMPLIANCE-AS-CODE | AI GOVERNANCE | CGE-P / CGE-AUD | ISO 27001 / 27701 / 42001 LEAD AUDITOR

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

PROFESSIONAL SUMMARY

GRC Engineer and Lead Auditor with 4+ years bridging governance requirements and technical enforcement. I ship compliance-as-code (Terraform baselines, OPA/Rego policy libraries with CI-gated enforcement, OSCAL control-to-code mapping, Cosign-signed evidence packs) and audit against what I build (ISO 27001 / 27701 / 42001 Lead Auditor + CGE-P and CGE-AUD). Currently co-leading AI governance adoption at HISPI's Project Cerebellum — 5+ client organizations assessed against NIST AI RMF and ISO 42001. Recent work includes HIPAA API governance pipelines with live credential-exposure remediation, EU AI Act classification engines that block deployment on governance failures, and RAG-based control framework lookup agents. Practitioner background across TPRM, SOC 2, ISRM, and framework gap assessments makes me equally credible in the audit room and the pull request.

CORE COMPETENCIES

GRC Engineering: Compliance-as-Code · Policy-as-Code (OPA/Rego) · Automated Evidence Collection · CI/CD Governance Gates · Control-to-Code Mapping · Machine-Readable Compliance (OSCAL) · Sealed Evidence Vaults · Signed CI/CD Pipelines · Cloud Compliance Automation (Terraform)

GRC Analyst & Audit: TPRM · Vendor Security Assessments · Security Questionnaire Response · SOC 2 Audit Support · Evidence Collection · Control Mapping · Risk Register & ISRM · Policy/Standard/Procedure Development · Internal Audit · Gap Assessment · Remediation Coordination · Executive Risk Reporting · GRC Platform Administration

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, 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.
- **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, United States

Mar 2024 – Jun 2024

- **Developed and maintained** security documentation, policies, standards, procedures, and runbook, 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%+**.

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

- Built a HIPAA Security Rule governance pipeline (Terraform + OPA/Rego + OSCAL + Cosign) for a patient-intake API: customer-managed KMS, S3 Object Lock evidence vault, multi-region CloudTrail, and 6 tested OPA/Rego policies.

- Assurance: Conftest fail-closed CI gate and Cosign keyless signing write evidence packs (including failing runs) into the vault, with OSCAL control-to-code mapping from HIPAA requirement through policy to artifact.
- Identified and remediated a live credential-exposure finding during hardening, including key rotation and repository hardening.

ARGUS — AI Governance Compliance-as-Code Engine

github.com/Toyeeb29/argus-ai-grc

- Built a Python CI-gated engine classifying AI systems under the EU AI Act against a control catalog crosswalked to NIST AI RMF and ISO/IEC 42001 (inventory → classification → evaluation → gate → evidence).
- GitHub Actions gate blocks merge on critical findings; each run produces sealed evidence (assessment report, findings register, Statement of Applicability, SHA-256 integrity manifest), including on failure.
- Puts AI governance on the same fail-closed CI path as infrastructure, critical governance failures stop deployment instead of becoming after-the-fact findings.

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 instead of free-form model output.
- Ingests framework text, embeds into Pinecone, and returns retrieval-backed answers with verified example queries against NIST SP 800-53 Rev. 5.
- Replaces manual control-catalog search with citable GRC knowledge automation for gap assessments and evidence mapping.

Multi-Cloud Compliance Lab

github.com/Toyeeb29/cgep-labs

- Built compliant-by-default Terraform modules with keyless OIDC / Workload Identity Federation across AWS and GCP, documented in OSCAL for machine-readable control intent.
- CI-passing lab for multi-cloud compliance automation, Org Policy / IAM posture patterns, and reusable evidence-oriented module design.
- Reference implementation mapping cloud control requirements to enforceable Terraform and identity-federation defaults.

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