John Kasonga – GRC Analyst Portfolio (Detailed, 2025)

Fort Worth, TX | 617-849-1247 | johnkasonga0572@outlook.com
LinkedIn: https://www.linkedin.com/in/john-kasonga-4ab914148/ | GitHub: https://github.com/JKASONGA1

Summary

Governance, Risk, and Compliance (GRC) analyst with strong documentation and policy development skills. Experienced in aligning technical controls with CIS, NIST, and ISO standards. Adept at producing compliance reports, security baselines, and risk assessments for technical and executive stakeholders.

Core Skills

• Governance & Documentation: Policy writing, compliance audits, security baselines
• Risk & Compliance: CIS benchmark alignment, NIST Cybersecurity Framework, ISO concepts
• Reporting: Executive summaries, remediation guidance, audit trail documentation
• Awareness & Training: Metrics reporting, phishing awareness programs
• Tools: Splunk, Linux/Windows hardening, Burp Suite, GoPhish, GitHub Actions (DevSecOps direction)

Detailed Projects

System Hardening & Compliance (BSC): Authored policies for PAM, sudo, and password standards. Conducted user/group access reviews and aligned results with CIS benchmarks. Produced compliance reports with remediation steps.

Incident Response Plan (TDIR-SBN): Developed a comprehensive IR plan including containment, eradication, recovery, and lessons learned. Mapped plan steps to NIST IR framework for audit readiness.

Web App Security with CI/CD (DevSecOps): Integrated Semgrep (SAST), OWASP ZAP (DAST), and Trivy (dependency scanning) in GitHub Actions; blocked PRs on high severity, fixed 3+ issues with commit diffs; added STRIDE threat model and SARIF outputs; produced CI badge and policy-as-code examples.

Email Security & Anti-Phishing Program: Ran 2–3 GoPhish campaigns; implemented SPF/DKIM/DMARC on test domain; built SOC playbook for reporting/triage; captured metrics and DMARC reports.