Luigi Carpio

Compliance Automation | GRC Engineer | Public Safety Technology
Sacramento, CA | klcarpio@gmail.com | (510) 316-2411 | GitHub | LinkedIn | luigicarpio.dev

SUMMARY

GRC Engineer with hands-on experience in CJIS-regulated and FedRAMP High environments serving law enforcement and public safety agencies. Background spans compliance-focused technical support for public safety SaaS platforms, identity governance and administration in financial services, and security operations in AWS and Azure environments. Builds open-source Python-based compliance automation tools including continuous monitoring pipelines, evidence collectors, and policy-as-code scanners mapped to CJIS v6.0, FedRAMP High, and NIST 800-53 Rev 5 controls.

TECHNICAL SKILLS

Automation & Scripting: Bash, Git/GitHub Actions, JSON/YAML, PowerShell, Python (boto3, compliance-trestle, oscal-pydantic), REST APIs

Cloud & Infrastructure: AWS (CloudTrail, Config, EventBridge, GovCloud, IAM, KMS, Lambda, S3, Security Hub), Azure (Entra ID, Policy, Sentinel), CloudFormation, Terraform

Compliance Operations: Access reviews, audit readiness, control mapping across frameworks, evidence collection and automation, privileged access monitoring, risk assessment

Frameworks & Standards: CJIS Security Policy v6.0, FedRAMP (High baseline), GovRAMP, NIST 800-53 Rev 5, NIST 800-171, NIST CSF 2.0

GRC & Security Tooling: Checkov, Conftest, IBM Compliance Trestle, Kibana/OpenSearch, OPA/Rego, OSCAL, Sentry, SIEM dashboards (KQL), Splunk

EXPERIENCE

Software Support Analyst II | *Mark43* May 2025 – Present

- Support mission-critical public safety applications operating under CJIS and FedRAMP High requirements, troubleshooting RBAC configurations, permission conflicts, and data handling across multi-tenant law enforcement environments.
- Investigate system issues using API testing, Kibana/OpenSearch log analysis, Sentry stack trace investigation, and SQL queries to trace data flows and identify root causes, producing evidence artifacts for incident documentation.
- Lead high-priority incident calls coordinating between law enforcement customers, engineering, and product teams while maintaining compliance with CJI handling requirements.
- Collaborate cross-functionally to resolve regulatory compliance issues across customer tenants, ensuring configurations meet CJIS and FedRAMP requirements.
- Develop AI-powered code analysis tools and a multi-language reading guide (Java, TypeScript, Gherkin, SQL) that enabled Support specialists to independently investigate application-level issues across the enterprise codebase, reducing reliance on engineering escalations.

Security Administration Analyst | *Mechanics Bank* May 2024 – May 2025

- Conducted privileged access reviews for 100+ high-risk applications, validating least-privilege enforcement and compliance with access control and authentication requirements.
- Performed security assessments across 300+ enterprise applications, producing remediation reports identifying risks in identity access controls and RBAC configurations.
- Automated directory and file management workflows using PowerShell, doubling team efficiency in recurring access review processes and evidence collection.
- Maintained security grids mapping user entitlements to role-based access policies, supporting internal audit evidence requirements and regulatory compliance.

Technical Support Specialist | *Axon Enterprise* Apr 2023 – May 2024

- Analyzed application and system logs using Splunk to identify anomalies and support incident investigations in a CJIS-regulated environment handling law enforcement digital evidence.
- Built a centralized knowledge base covering 40+ public safety products, improving team response efficiency for compliance-sensitive support scenarios.
- Troubleshot and resolved issues across digital evidence and records management platforms, ensuring system reliability and data availability for law enforcement agencies operating under CJIS requirements.

Cybersecurity Support Analyst (Intern) | *LOG(N) Pacific* Dec 2022 – Sep 2023

- Configured secure cloud environments using Azure tools aligned to NIST compliance frameworks, including Entra ID, Sentinel, and Azure Policy.
- Developed KQL queries and SIEM dashboards for security monitoring and threat detection, producing compliance-relevant telemetry for audit evidence.

PROJECTS

Open-source compliance automation tools: github.com/0xBahalaNa | luigicarpio.dev

- **AWS Compliance-as-Code:** CloudFormation templates and SCPs enforcing FedRAMP High security baselines for automated, compliant resource deployment.
- **Compliance Evidence Collectors (Python/boto3):** Automated audit tools for CloudTrail, IAM, S3, and Security Groups generating structured JSON evidence mapped to CJIS v6.0, FedRAMP High, and NIST 800-53.
- **Continuous Monitoring Pipeline:** Event-driven compliance monitoring using AWS Config, Lambda, and SSM with auto-remediation for configuration drift.
- **NIST 800-53 Rev 5 to AWS Service Mapping:** Control-by-control documentation with OSCAL Component Definition JSON output aligned to FedRAMP 20x machine-readable evidence requirements.
- **Policy-as-Code Scanner:** Terraform plan validation integrating Checkov and OPA/Rego policies for CJIS v6.0 and FedRAMP High compliance checks in CI/CD pipelines.
- **Secret Scanner:** Recursive directory scanner for exposed credentials with CI/CD gating via non-zero exit codes, mapped to IA-5(7), SC-12, and SC-28.

EDUCATION

Bachelor of Science, Criminal Justice California State University, Sacramento
Bachelor of Science, Cybersecurity and Information Assurance Western Governors University

CERTIFICATIONS

ISC2 Systems Security Certified Practitioner (SSCP)
CompTIA CySA+, PenTest+, Security+, Network+, A+, Project+
ITIL 4 Foundations
LPI Linux Essentials