

Luigi Carpio

Compliance Automation | GRC Engineer | Public Safety Technology

lcarpio@gmail.com | (510) 316-2411 | [GitHub](#) | [LinkedIn](#) | [luigicarpio.dev](#)

Open to Remote | Active Public Trust Clearance (U.S. Department of the Interior) | U.S. Citizen

SUMMARY

GRC Engineer and former law enforcement officer building compliance automation for CJIS v6.1 and FedRAMP High environments. Active Public Trust clearance (U.S. Department of the Interior). Current role supports a FedRAMP High public safety platform serving law enforcement agencies; open-source work ships the tooling those environments need: OSCAL Assessment Results shaped for FedRAMP 20x, an audit-evidence warehouse with population-completeness tests, and CloudFormation/SCP baselines enforcing FedRAMP High, all mapped to NIST 800-53 Rev 5. AI agent workflows accelerate the builds, with a separate model auditing every diff before commit. Identity governance foundation from financial services: access certifications across 300+ enterprise applications. SSCP plus six CompTIA certifications.

TECHNICAL SKILLS

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

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 v6.1, 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

GRC Engineer | *Independent Open-Source Compliance Automation* 2024 – Present

- Built and shipped 11 open-source compliance automation tools across CJIS Security Policy v6.1, FedRAMP High, NIST 800-53 Rev 5, SOC 2, and ISO 27001:2022, each with CI gates that block control and artifact drift.
- Federal flagships: Evidence Warehouse treating audit evidence as a data product (dbt/DuckDB, per-source data contracts, completeness tests that fail the build); OSCAL Evidence Pipeline emitting FedRAMP 20x-shaped machine-readable Assessment Results; AWS Compliance-as-Code enforcing FedRAMP High baselines with CloudFormation and SCPs.
- Commercial flagships: SOC 2 / ISO 27001 / NIST 800-53 unified controls crosswalk with a drift-blocking CI gate; Security Questionnaire Responder that cites the criterion behind every answer and abstains on anything it cannot ground; Vendor Security Due Diligence scoring residual risk from data classification and production access.
- Tooling: Python (boto3, oscal-pydrantic, compliance-trestle), dbt, DuckDB, CloudFormation, OSCAL, GitHub Actions, MCP servers; AI agent workflows where one model writes the code and a separate model audits the diff before commit.

Support Specialist – CJIS / FedRAMP High Public Safety Platform | *Mark43* April 2026 – Present

Software Support Analyst II – CJIS / FedRAMP High Public Safety Platform | *Mark43* May 2025 – April 2026

- 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 – Identity Governance & Access Reviews | *Mechanics Bank* May 2024 – May 2025

- Executed recurring user access review and privileged access certification campaigns across 100+ high-risk applications, pre-building population and entitlement views for application owners and managers to keep certifications on schedule and validating least-privilege against documented access control requirements.
- Caught stale application-owner entitlement exports three times in a single review cycle and repointed population pulls to the system of record, protecting completeness and accuracy of certification evidence; annual cycle closed with zero internal audit findings.
- Performed access and security assessments across 300+ enterprise applications, producing certification reports and remediation documentation identifying risks in identity access controls, Active Directory group membership, and RBAC configurations.
- Automated recurring review-cycle preparation and evidence collection with PowerShell, scaffolding the review directory structure for all 100+ applications and roughly doubling team throughput on certification cycles.

Technical Support Specialist – Law Enforcement Digital Evidence (CJIS-Regulated) | *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.
- Troubleshooted 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.

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