Keith Loparnos

Staten Island, New York, 10314 | 917-418-1607 | keith.loparnos@yahoo.com |

LinkedIn Profile | GRC Portfolio - GitHub

Professional Summary

Detail-oriented cybersecurity and compliance professional transitioning into Governance, Risk, and Compliance (GRC), with more than 25 years of leadership and operations experience. Holds a Bachelor of Science in Cybersecurity with a 4.0 GPA and Summa Cum Laude distinction, along with a Bachelor of Science in Finance. CompTIA Security+ and ISC2 Certified in Cybersecurity (CC). Hands-on experience in risk assessments, control mapping, compliance documentation, security frameworks, remediation planning, and evidence analysis through cybersecurity projects and practical GRC work.

Education

Bachelor of Science in Cybersecurity
Purdue University Global — December 2025

- 4.0 GPA
- Summa Cum Laude

Bachelor of Science in Finance
St. John's University — September 2005

Certifications

CompTIA Security+ (SY0-701) — June 2026

ISC2 Certified in Cybersecurity (CC) — April 2026

CompTIA CySA+ (CS0-004) — Currently Pursuing

GRC & Cybersecurity Skills

Risk Assessments • Risk Registers • Control Mapping • Gap Assessments • Remediation Planning • Compliance Documentation • Audit Evidence • Governance Reporting • NIST CSF 2.0 • NIST SP 800-53 • ISO/IEC 27001 • Linux and Windows • Nessus • Nmap • Splunk • Security Onion • Wireshark • VirusTotal • Autopsy and EnCase • Python • Metasploit • John the Ripper

Projects

GRC Risk Assessment & Control Mapping | Tri-State Financial Services

- Developed an asset inventory and risk register to identify, assess, and prioritize cybersecurity risks within a fictional financial services environment.
- Mapped identified risks to applicable security controls using NIST CSF 2.0 and ISO/IEC 27001, documenting control objectives and implementation considerations.
- Performed a GRC gap assessment comparing current and desired security states and developed a remediation plan with priorities, responsible owners, target timeframes, and success criteria.
- Created an ISO/IEC 27001 Statement of Applicability (SoA) documenting control applicability, justification, implementation status, responsible owners, and evidence references.

Incident Response Planning

- Developed a customized enterprise Incident Response Plan aligned with NIST SP 800-61 Rev.2 – Computer Security Incident Handling Guide.
- Translated incident response requirements into documented procedures, roles, responsibilities, and escalation workflows.
- Coordinated security, legal, management, vendors, and business stakeholders to support incident response planning, documentation, and operational readiness.

Organizational System and Application Security Procedures

- Developed and standardized an organizational-wide cybersecurity policy framework covering access control, incident response, data protection, risk management, and compliance.
- Mapped cybersecurity policies and controls to NIST CSF 2.0, NIST 800-53, and ISO/IEC 27001 requirements to support compliance and audit readiness.
- Established a governance process for maintaining current, enforceable policies and procedures aligned with business requirements and security objectives.

Bachelor's Capstone in Cybersecurity | Incident Response Team

- Collaborated with a 5-person incident response team to manage a high-severity simulated worm and DDoS event in alignment with NIST SP 800-61 Rev. 2 guidelines.
- Supported containment, eradication, and recovery efforts by isolating affected systems, updating firewall rules, and applying DDoS mitigation controls to limit business impact.
- Assessed and classified the incident based on severity and operational risk, ensuring response actions follow organizational policy and compliance standards.
- Co-authored a concise employee notification outlining outage details, device isolation instructions, and help desk escalation procedures to maintain clear communication during the incident.

Professional Experience

Operations Manager | JGL Fine Foods, Inc. | Brooklyn, NY **1997 – Present**

- Directed daily business operations for a high-volume retail environment processing 6,000+ monthly transactions while maintaining zero data breaches.
- Implemented and enforced payment security and data-handling controls to protect customer credit card information and meet compliance standards such as PCI-DSS.
- Increased revenue by 10% by launching new products and services while aligning operations with customer demand.
- Led, trained, and supervised a diverse team, and created standardized procedures to ensure consistent policy adherence and service quality.
- Developed internal controls for inventory, cash handling, and vendor access to reduce operational risk.
- Managed regulatory compliance and maintained audit-ready documentation.
- Coordinated with accountants and external vendors to ensure accurate financial reporting.
- Resolved operational incidents and maintained business continuity during staffing shortages, equipment failures, and supply disruptions using risk-based decision making.