

NICK SOTIROGLOU

GOVERNANCE, RISK & COMPLIANCE | CISA

Lincolville, South Carolina | 843-693-4124 | nsotiroglou@gmail.com

linkedin.com/in/nicholas-sotiroglou | nicksotiroglou.com

SUMMARY

CISA-certified governance, risk, and compliance professional who has built and run GRC programs across technology organizations. Experience spans security risk assessments, third-party risk management, policy governance, customer assurance, and audit readiness across SOC 2, ISO 27001, PCI DSS, and HIPAA-related requirements. Brings a product delivery and QA background to translating security requirements into practical controls, clear ownership, and remediation.

CORE SKILLS

Program governance: GRC program development and ownership; policy management; cross-functional delivery.

Risk and assurance: Security risk assessments; third-party risk management; customer security reviews; remediation management.

Audit and controls: External audit readiness; control mapping; evidence review; gap analysis.

Framework experience: SOC 2, including Type II; ISO 27001; PCI DSS; HIPAA-related requirements. Familiarity: NIST CSF, GDPR, CCPA/CPRA.

Tools: OneTrust, Vanta, Jira, Confluence, ServiceNow, SQL.

PROFESSIONAL EXPERIENCE

11:11 Systems | Compliance & Audit Specialist

Mar 2023 - Present

- Built and ran the GRC program, establishing priorities, ownership, and recurring workflows across risk management, policy governance, third-party assurance, customer reviews, and audit readiness.
- Conducted security risk assessments and translated identified gaps into prioritized remediation with defined owners, target dates, and follow-up.
- Managed third-party risk reviews, evaluated vendor security information, and coordinated follow-up on identified concerns.
- Owned policy governance, coordinating policy development, reviews, and updates with responsible stakeholders.
- Managed customer assurance work, translating security policies and control evidence into clear responses to customer security and compliance inquiries.
- Led external audit coordination across SOC 2, ISO 27001, and PCI DSS, managing auditor requests, evidence submissions, control-owner follow-up, and remediation.
- Mapped framework requirements to controls, evidence expectations, and owners; reviewed control evidence and documented gaps requiring follow-up.
- Used OneTrust to organize control evidence and validate completeness; maintained remediation ownership, due dates, and status across recurring compliance work.

ThreeFlow | Product Delivery Manager

Dec 2021 - Feb 2023

- Built and ran the GRC program alongside product delivery responsibilities, connecting risk, policy, vendor and customer assurance, and audit readiness with engineering execution.
- Led audit coordination for SOC 2 Type II and HIPAA-related requirements, translating control and evidence needs into delivery plans and implementation follow-up.
- Conducted risk assessments and vendor security reviews; translated identified gaps into Jira work items with acceptance criteria, dependencies, ownership, and follow-up.
- Managed policy review and update workflows and addressed customer security inquiries using relevant policy and control evidence.
- Managed Vanta-supported workflows for security requirements, evidence needs, ownership, and implementation status; tracked unresolved risks and blockers affecting audit readiness.

ThreeFlow | Project Management Operations Specialist

Jun 2021 - Dec 2021

- Built support workflows covering SLA tracking, service-desk configuration, documentation, training, and handoffs; coordinated product rollouts and user-acceptance testing.

Ceterus | QA Engineer Team Lead

Dec 2019 - Jun 2021

- Led manual and automated QA, coordinating regression coverage, defect follow-up, and release validation with engineering; supported non-production releases through Jenkins and CircleCI.

Ceterus | QA Engineer

May 2019 - Dec 2019

- Created test plans, documented reproducible defects, and used SQL to validate application data and investigate issues.

Ceterus | Technical Support Specialist

Feb 2018 - May 2019

INDEPENDENT PROJECT

Kasbah Labs | GRC Workflow Application

Jun 2025 - Apr 2026

- Designed, built, deployed, and maintained an independent application connecting control ownership, evidence uploads, policy acknowledgments, remediation tracking, and audit preparation.

CERTIFICATION

Certified Information Systems Auditor (CISA) | ISACA | Mar 2026

EDUCATION

Bachelor of Science, Information Technology | Western Governors University | 2021