

# Richard Vincent

## Cybersecurity Professional | Governance, Risk & Compliance (GRC) | Security Operations

Atlanta Metropolitan Area | LinkedIn: [linkedin.com/in/richvince](https://www.linkedin.com/in/richvince) | Portfolio: [richvince.github.io](https://richvince.github.io)

### PROFESSIONAL SUMMARY

Cybersecurity professional with 9+ years of IT infrastructure, enterprise support, and technical operations experience, currently transitioning into Governance, Risk & Compliance (GRC) and cybersecurity analysis. Experienced in network support, troubleshooting, documentation, security investigations, and risk-focused analysis across operational environments. Developed portfolio work involving audit reporting, control assessments, risk documentation, phishing investigations, Windows log analysis, and security operations workflows aligned with NIST CSF and ISO 27001 concepts.

### CORE COMPETENCIES

**Governance, Risk & Compliance:** Risk Assessment • Security Controls • Audit Support • Compliance Documentation • Control Gap Identification • Remediation Planning

**Frameworks & Concepts:** NIST CSF • ISO 27001 Concepts • CIS Controls • Governance Support • Incident Response Support • Security Operations Workflows

**Tools & Technical Exposure:** Windows Event Viewer • Splunk • Wazuh • Wireshark • Network Security • Technical Documentation

### PROFESSIONAL EXPERIENCE

**Senior IT Network Technician** | Interconnexion Point Limited | 2020–2023

- Supported enterprise networking and IT infrastructure operations in production environments, helping maintain operational reliability and structured issue resolution processes.
- Assisted with troubleshooting network connectivity, user support, system administration tasks, and technical issue documentation across business environments.
- Worked within structured operational processes that required consistency, escalation awareness, and technology governance discipline.
- Built transferable experience relevant to control awareness, audit support, technical documentation, and risk-informed operational review.

**IT Infrastructure / Technology Support Experience** | Additional experience contributing to 9+ years total

- Supported technical environments requiring troubleshooting, service continuity, issue tracking, and user-facing support.
- Developed practical experience in documentation, systems support, and structured problem-solving that translates well into GRC and cybersecurity analysis work.

### TRAINING & CERTIFICATIONS

- CompTIA Security+ (In Progress)
- Per Scholas Cybersecurity Program
- Splunk Core User Training
- Cisco Network Defender Training
- Planned Next-Step Training: GRC Mastery

### PORTFOLIO HIGHLIGHTS

Security Audit Report Collection • Risk & Control Assessments • Windows Security Log Investigation • Enterprise Phishing Investigation • Brute Force Login Investigation • DNS Client Log Investigation • Network Incident Investigation

### TARGET ROLES

GRC Analyst • Security Compliance Analyst • Cyber Risk Analyst • IT Audit Associate • Third-Party Risk Analyst • Information Security Analyst