

Alexander Dabbs

Seattle, Washington | alexdabbs@me.com | (813) 362- 6454 | www.linkedin.com/in/alexander-dabbs

Website: alexdabbs.com | GitHub: github.com/alex-dabbs

PROFESSIONAL SUMMARY

Security Risk Assessor with 4+ years of specialized experience in third-party risk management, control assessments, and regulatory compliance across energy and utility sectors.

SKILLS

Security: SIEM, Encryption Methods, SBOMs, Risk Management Assessments, Incident Response

GRC Tools: ServiceNow, JIRA, Proprietary Company TPRM Platforms.

Risk Management: Risk Assessment Frameworks (NIST RMF, ISO 27001, SOC 2 Type II, NIST 800-218, NERC/CIP), Quantitative & Qualitative Risk Analysis, Breach Impact Analysis, GRC Program Development.

Languages and Technologies: Python, JavaScript, React, Vite, HTML/CSS.

PROFESSIONAL EXPERIENCE

Security Risk Assessor | Fortress Information Security | Orlando, FL (Remote)

April 2026 - October 2026

- Primary risk assessor across three Fortune 500 regulated utility companies and a federally-owned utility.
- Managed cloud security, AI governance, and product development assessments, security supplements, and risk ranks collaborate with legal, engineering and privacy teams to maintain deliverables and document remediation reports.
- Conducted third-party security risk assessments for external auditing (30+/-month) against NIST, SOC 2, and ISO 27001 requirements to evaluate compliance and effective controls across access management, change management, data protection, business continuity, and network security categories.
- Delivered annual risk reports to leadership and client governance teams, highlighting exposures and control gaps across 750+ security findings to prioritize remediation.
- Designed and drove the implementation of automated configuration monitoring processes to validate preliminary risk ratings against preapproved scoring methodologies, determine inherent risk, and standardize third-party vendor risk assessments.
- Led implementation of AI-powered evidence analysis within a proprietary GRC platform, reducing evidence review time from two hours to 45 minutes per review, while automating preliminary findings allocation and retaining analyst validation to identify false positives.

Security Risk Analyst | Fortress Information Security | Orlando, FL (Remote)

February 2024 - April 2026

- Primary liaison between the organization and third-party vendors, driving remediation of 120+ high-risk findings monthly through actionable POA&Ms, 90-day remediation deadlines, and midpoint progress reviews, improving vendor response rates by 65% and accelerating risk reduction.
- Developed and implemented risk scoring automation procedures cutting processing time by 30 minutes per record (20%), improving throughput and boosting monthly projection capacity by 25%.
- Contributed to over 300+ yearly Software Bill of Materials (SBOMs) and Software Attestation projects for public and federal utility companies, to ensure NIST 800 compliance and enhance software security measures.
- Improved organizational risk posture by collaborating cross-functionally with client business units to develop risk treatment plans and control mitigation, contributing to policy and standards development.
- Evaluated SOC 2 Type II Reports and ISO 27001 certifications, map vendor controls to multiple client compliance requirements, and calculated inherent risk scores to execute comprehensive third-party risk assessments.

Senior Cybersecurity Research Analyst | Fortress Information Security | Orlando, FL August 2023 - February 2024

- Determined weakness in domain configuration and security flaws by leveraging OSINT and proprietary tools to conduct 25+ quantitative risk management assessments per month for energy and utility clients.
- Improved and tested internal program plans to increase reliability and accuracy of AI-centered procedures through source verification and lineage reviews, input validation stress tests, and reproducibility testing.
- Monitored and analyzed company-owned and prospective domains to detect and flag malicious, explicit, or brand-damaging content, ensuring compliance with security and reputational standards.

Cybersecurity Research Analyst | Fortress Information Security | Orlando, FL

February 2023 - August 2023

- Collected data using public, private, and proprietary tools related to ERAI, GDPR, security incidents, and product vulnerabilities to gauge vendor compliance and determine potential risk.
- Recorded security incident responses, non-compliance with GDPR, HIPAA, CMS and PCI-DSS, and improper domain security configurations into consolidated reports enabling clients to proactively address vendor risks.

EDUCATION

Florida State University | Tallahassee, FL | *Bachelor of Science, Psychology*
University of Central Florida | Orlando, FL | *Cybersecurity Defense Professional*

PROJECTS

GRC Workflow Portfolio

September 2026 - October 2026

- Conducted an ISO/IEC 27001:2022 gap assessment across five security control areas for a simulated critical-infrastructure environment, evaluating access control, authentication, network security, web-filtering, and incident response preparedness.
- Identified and documented security control gaps, potential vulnerabilities, and risk exposure affecting cloud hosted-SCADA infrastructure, AI workloads, and operational technology (OT) environments.
- Developed a security findings and remediation tracker with risk ratings, accountable stakeholders, proposed remediation timelines, and evidence-based closure criteria to support risk treatment and compliance monitoring.
- Produced an executive summary translating technical security findings into actionable remediation recommendations, incorporating relevant NERC CIP considerations and ongoing control assurance practices.

Risk Rating Dashboard

October 2026

- Developed a React-based GRC Risk-Rating dashboard to centralized ISO 27001:2022 security findings, control references, evidence documentation, and remediation tracking.
- Implemented risk distribution and residual risk visualizations to support risk management, prioritization, and visibility into remaining security exposure.
- Built interactive findings management functionality, including risk and status filtering, due-date sorting, ownership tracking, overdue identification, and remediation status updates.
- Engineered persistent browser-based findings storage and record management capabilities to maintain assessment data, track updates, and support ongoing security remediation workflows.

Computer Networking with CISCO

July 2024

- Developed a Wide Area Network (WAN) for a mock bank that included three Local Area Networks (LAN), one of which was partitioned using a VLAN and configured all network devices and endpoints to communicate to the entire WAN.
- Designed an IP Address Scheme and implemented VLANs and Trunking Protocols and assigned IP addresses to each subnet and configured specific routers for Inter-VLAN routing.
- Secured switch physical ports and configured OSPF and Extended ACLs to prevent guests on the network from connecting to the NTP/Syslog Server.
- Configured settings to prevent unauthorized access and enabled secure remote access through SSHv2 on all routers.

AWS Cloud Security Instancing

April 2024

- Utilized AWS to create an EC2 instance with basic configuration to connect via RDP and implemented IAM features for user and group creation and modified existing groups to govern ICMP and RDP access to AWS resources.
- Created a virtual Windows Server 2012 R2 machine with basic configuration settings and enabled Inspector to improve instance security.
- Established an organization within the instance to allow for centralized management for multiple AWS accounts and created service control policies with security verification.
- Configured an S3 Bucket with a file and CloudFront to deliver the contents of the file and configured WAF to control which traffic from the application will be permitted or blocked according to the rules set.