Jesselyn West

864-776-2669 | jesselynmwest@outlook.com | LinkedIn

RISK & COMPLIANCE ANALYST

Dynamic and highly motivated professional transitioning from a successful career in food service management to the field of cybersecurity. Brings a unique blend of exceptional customer service skills, problem-solving abilities, and a strong commitment to maintaining confidentiality and security protocols. Recognized for an acute attention to detail, quick adaptability in fast-paced environments, and a collaborative approach to team-based tasks. Recent educational pursuits in cybersecurity, including certifications and self-directed learning, demonstrate a genuine passion and growing expertise in data protection, risk assessments, and digital security practices.

- Risk Assessments
- Compliance Auditing
- Security Risk Documentation
- Regulatory Alignment
- Stakeholder Engagement
- Control Testing

Technology Proficiencies

Frameworks: NIST 800-53, ISO 27001/27002, DISA STIG, Risk Management Framework (RMF), Cybersecurity Framework (CSF), CIS Controls, PCI DSS, HIPAA, GDPR, SOC 2, ITIL, NIST SP 800 series

Software: Microsoft Sentinel, Tenable.io, Defender for Endpoint, Azure Virtual Machines, KQL, PowerShell, Nessus, Qualys, ServiceNow, Splunk, AWS Security Hub, Jira, IBM QRadar, Wireshark, SecureAuth-AD, Palo Alto XSOAR, RSA Archer, ServiceNow GRC, SharePoint,

Cloud: Microsoft Azure, AWS

Scripting: Python, Bash, Powershell, JavaScript

Networking: OSI, TCP/IP, Firewalls, IDS/IPS, LAN, Mesh Wi-Fi Network Systems, DHCP, VPN, DNS

PROFESSIONAL DEVELOPMENT

United Airlines | **Compliance & Cloud Security**

- Collaborated in a structured governance and compliance cohort focused on risk, audit, and cloud security practices in a regulated enterprise environment.
- Performed control mapping exercises aligning NIST CSF and CIS Controls to cloud services (Azure, Microsoft 365), identifying compliance gaps and proposing remediation steps.
- Assisted in policy review and update simulations, ensuring documentation met audit-readiness standards for HIPAA and ISO 27001.
- Conducted a risk analysis workshop using scenario-based methods (likelihood/impact scoring) to prioritize cloud security threats and recommend treatment options.

Work Experience

Axis Security Solutions | Remote — 8/2025 – Present

Jr. GRC Analyst

- Map business processes and existing safeguards to NIST 800-53, NIST CSF, PCI-DSS, HIPAA, and FISMA; document control coverage, gaps, and compensating controls.
- Support risk assessments by drafting risk statements, scoring likelihood and impact, proposing treatments, and updating the risk register with owners and due dates.
- Execute evidence collection for audits and customer questionnaires; maintain audit-ready folders, chain-of-custody notes, and traceable links to control IDs.
- Perform periodic access governance reviews (least privilege, SoD checks, stale-account remediation, MFA coverage) and track exceptions through closure.
- Coordinate CA-8-aligned security testing activities (scope, ROE artifacts, completion evidence) and report remediation status and control effectiveness to stakeholders.

Cigna | Remote — 9/2022 – Present

Lead Revenue Compliance Analyst

- Executed control testing and monitoring of revenue cycle processes, validating compliance with HIPAA, CMS, and SOC 1/SOX-relevant controls, ensuring accuracy and defensibility of billing operations under regulatory scrutiny.
- Authored and maintained governance artifacts (policies, SOPs, risk registers) and mapped them to NIST CSF and internal compliance frameworks, strengthening audit evidence packages for both internal and external assessors
- Conducted risk assessments in alignment with NIST SP 800-30 by identifying threats (e.g., data integrity failures, coding errors), evaluating likelihood/impact, and recommending risk treatment strategies with mitigation tracking
- Partnered with various stakeholders to design data validation and reconciliation controls, reducing residual risk from billing discrepancies and improving assurance over financial reporting integrity.
- Facilitated remediation and POA&M tracking for identified compliance gaps, ensuring issues were documented, prioritized by risk appetite, and closed with verifiable evidence of effectiveness

NEWREZ **|** Remote 1/2020 – 9/2022
Risk & Compliance Officer

- Performed end-to-end compliance reviews of loan origination and servicing files, applying risk-based audit planning principles to assess control coverage against federal lending standards, CFPB guidance, and internal risk tolerance
- Designed and executed evidence collection workflows (document sampling, control walkthroughs, exception testing) to ensure defensible audit trails and continuous readiness for regulatory examinations
- Produced quantitative and qualitative risk analysis of loan portfolio exposures, leveraging scenario-based assessments to highlight vulnerabilities and support executive decision-making in risk treatment planning
- Drafted corrective action plans aligned to ISO 27001 risk treatment methodology, ensuring remediation efforts were traceable, measurable, and closed with control effectiveness validation

BLACK GIRLS HACK **|** Remote 9/2024 – Present
Technology Program Assistant Coordinator

- Own the governance calendar for training programs (session approvals, sign-offs, checkpoints) and maintain an artifact library (policies, SOPs, agendas, attendance, consent forms) so activities have a traceable audit trail and are easy to retrieve during reviews.
- Run lightweight evidence management: standard file naming and versioning, change logs for updates, and simple retention schedule for training records to support consistent documentation practices
- Support access governance for shared drives and folders (Google Drive): provision least-privilege by role, coordinate quarterly access reviews with program leads, remove stale access, and document approvals for transparency.
- Draft participant communications and post-event minutes that record decisions, owners, and due dates; track follow-ups to closure to keep the program in continuous readiness for internal or partner audits.

EDUCATION & CREDENTIALS

- CompTIA Security+ ce
- CompTIA A+
- ISC2 Certified in Cybersecurity
- Certified Information Security Auditor (CISA) (in progress)

Bachelor of Science in Psychology
UNIVERSITY OF SOUTH CAROLINA

Executive MBA
JACK WELCH MANAGEMENT INSTITUTE

Bachelor of Science in Cybersecurity & Information Assurance
WESTERN GOVERNORS UNIVERSITY (IN PROGRESS)