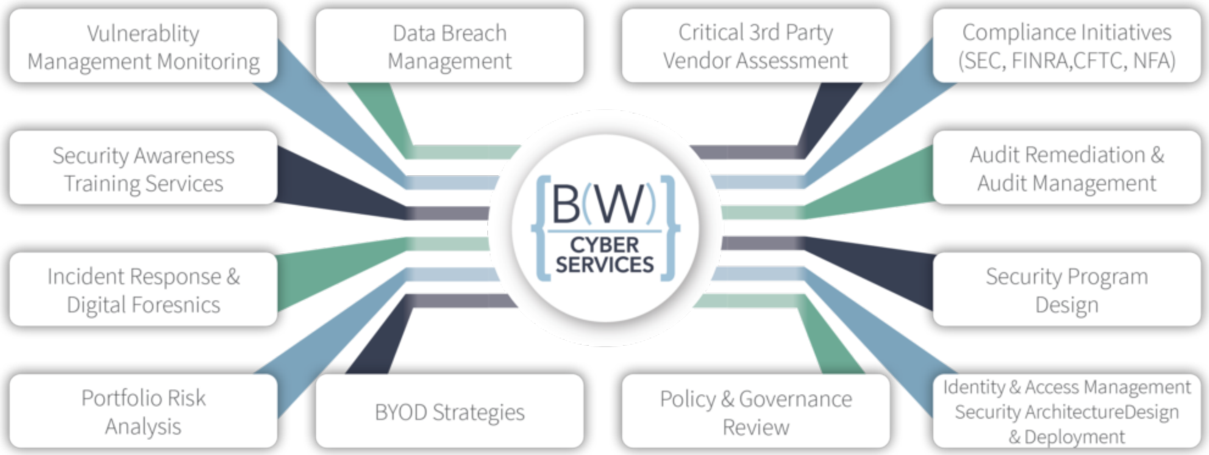
{B(W)} CYBER SERVICES
COMPLEXITY SIMPLIFIED

# Cybersecurity Risk Assessor

## About BW Cyber Services

BW Cyber Services is a Veteran Owned/Veteran Friendly industry-leading cyber security consultancy providing targeted solutions to highly regulated industries. As an industry leader, our blue chip consultants understand the unique nexus between cybersecurity, operational risk, and regulatory compliance. As depicted below, BW Cyber Services offers a full spectrum of security services that include testing, assessments, compliance, education, policy, forensic and virtual Chief Information Officer outsourcing.


Vulnerablity Management Monitoring
Data Breach Management
Critical 3rd Party Vendor Assessment
Compliance Initiatives (SEC, FINRA,CFTC, NFA)
Security Awareness Training Services
B(W) CYBER SERVICES
Audit Remediation & Audit Management
Incident Response & Digital Foresnics
Security Program Design
Portfolio Risk Analysis
BYOD Strategies
Policy & Governance Review
Identity & Access Management Security ArchitectureDesign & Deployment

BW Cyber Services provides extremely competitive compensation packages along with exceptional benefits (medical, 401k, vacation, etc.). We seek self-starters who are willing to learn quickly, work hard, and provide solid leadership by example. For additional information, please see our website at www.bwcyberservices.com, follow us on LinkedIn.com or contact us at info@bwcyberservices.com.

## Position Description – Cybersecurity NIST Risk Assessor

BW Cyber Services is seeking to hire a Cybersecurity NIST Risk Assessor who will plan and lead cybersecurity National Institute of Science and Technology (NIST) Risk Assessments to determine the overall security posture of BW Cyber Services' clients' operations. These assessments will include on-premises and cloud-based infrastructure as well as the critical 3rd party vendors supporting these clients. Candidates should be have strong understanding for cybersecurity requirements associated with regulated cybersecurity operations and related risk assessment for organizations that may include the Security Exchange Commission (SEC), the National Futures Association (NFA), the Federal Risk and Authorization Management Program (FedRAMP), the Health and Information Portability Accountability Act (HIPPA), etc. The risk assessments assigned to the Cybersecurity Risk Assessor will require a solid understanding of both general and technical controls in an IT environment. The Cybersecurity Risk Assessor will be required to use pre-defined processes, standards, and guidelines which will be applied consistently in the review of operations. Ultimately, using pre-defined templates, the Cybersecurity Risk Assessor will be required to create professional Risk Assessment reports, security enhancement suggestions, and audit findings/recommendations in a prioritized manner at the conclusion of the Risk Assessment.

During audits, the Cybersecurity Risk Assessor will interact with all levels of client personnel from IT and security line staff to C-level executives, as well as to present findings and recommendations to audit committees and/or senior management. During the various cybersecurity consulting engagements, the position will require the Cybersecurity Risk Assessor to quickly learn the client's business and operational environment in order to recommend pragmatic cybersecurity solutions, draft security programs, and related organizational compliance solutions that align with all applicable security standards, laws, and industry regulations.

Depending on the leadership skills of the selected candidate, position may be expanded to grow and manage a team of lesser experienced audit staff or other personnel assigned to support risk assessments. Ultimately, The Cybersecurity Risk Assessor will be expected to enhance and protect organizational value by providing stakeholders with risk-based, independent, objective, and reliable assurance, advice, and insight.

**Essential Duties and Responsibilities**

- Perform IT Risk Assessments and audits for customers against Cybersecurity Regulations and Standards
- Address industry-unique cybersecurity regulatory compliance requirements
- Manage all aspects of the audit lifecycle (e.g., perform risk assessment and control identification, finalize scope, lead walkthroughs, conduct testing, oversee assigned staff, review documentation, validate exceptions, and communicate results of testing)
- While initial training and oversight will be provided, the goal is for the risk assessor to independently conduct audits for small and mid-size commercial organizations in the financial services, healthcare, and legal industries with minimal supervision
- Provide recommendations and guidance on identified security and control risks
- Responsible for documenting methodology, findings, and recommendations to support Cybersecurity Risk Assessments and Audits
- Provide clients with recommendations for revisions to IT security policy and/or procedures when appropriate
- Develop, review, and update customer business resiliency plans (e.g., disaster recovery, business continuity, pandemic planning, incident response planning)
- Participate virtually in team projects and assignments
- Support integrated client activities as a member of an outsourced virtual IT Security officer (e.g., vCISO) team
- Conduct security awareness training for the client (performed virtually)
- Assist management in improving services and deliverables and suggesting new opportunities
- Prepare and deliver final documentation to support audit work with evidence of deficiencies in controls, duplication of effort, extravagance, fraud, or lack of compliance with laws, government regulations, and management's policies or procedures. Deliverables must comply with industry standards. (e.g., organized, clear, sufficiently detailed, able to articulate complex aspects of testing).
- Write clear and effective audit findings with limited supervision and assistance
- Effectively manage multiple assignments concurrently
- Makes presentations to various groups and departments on controls, audit findings, and recommendations
- Train/manage less experienced audit personnel in audit routines and conducting audit reviews
- Maintain good working relationship with all staff and clients to foster an open dialogue

- Performs all other job duties as assigned by supervisor

**Essential Requirements**

- Deep experience with NIST Control Assessment and related Risk Assessment activities for highly regulated industries
- Strong verbal and written communication skills
- Ability to work independently
- Comfortable working in a team environment
- Strong analytical and problem-solving skills
- Strong understanding of physical IT network infrastructure
- Strong awareness of current cybersecurity and hacking trends with a commitment to continuous learning to stay current regarding applicable strategies and regulatory and legal requirements
- Knowledge of or experience dealing with IT Regulations and Standards associated with NIST and CIS
- Experience with Policy and Procedure development
- Experience with Business Continuity Planning and Disaster Recovery
- Ability to manage multiple projects and schedules independently
- Knowledge of operating systems, network architecture, web development
- Cloud security experience (e.g., Azure, AWS, Google) a plus

**Desirable Requirements**

- 5+ years of full-time dedicated experience leading cybersecurity audits focused on delivering common sense recommendations designed to reduce risk
- Understanding of Industry trends in cloud technologies for public, private, and hybrid cloud deployments
- Bachelor’s degree in Computer Science, Engineering, Mathematics, related field; or equivalent combination of education/professional experience in a similar role
- One or more technical security certifications is a plus:
    - CISSP – Certified Information Systems Security Professional
    - CISM – Certified Information Security Manager
    - CCSP – Certified Cloud Security Professional
    - CSEC – SANS CIAC Security Essentials