Cybersecurity Governance Risk Compliance (GRC) Analyst

Position Details

Date of issue: March 2026
Position number: 00021560
Department and Campus: SITIS, University Services
Workplace Location: Remote
Collective Bargaining Unit (CBU): UMPSA
Job family and Wage grade: 1-Information Technology, Grade 06
Essential Employee: Yes
Fair Labor Standards Act (FLSA): Exempt

Primary Purpose of Position

The Cybersecurity Governance, Risk, Compliance (GRC) Analyst is responsible for supporting and advancing the University of Maine System's cybersecurity governance framework, risk management processes, regulatory compliance obligations, and security awareness programs. This role coordinates institutional cybersecurity policy development, risk tracking, compliance readiness, and program reporting to help ensure the confidentiality, integrity, and availability of university information systems and data.

The position works collaboratively with Information Technology, academic departments, administrative units, and external partners to assess risk, maintain compliance with regulatory and contractual requirements, manage audit readiness, and promote a strong culture of security awareness across the University community.

Essential Duties

1. Manage the institutional cybersecurity risk program, including maintaining the risk register, documenting risk, tracking mitigation plans, coordinating corrective actions, and supporting enterprise risk management activities.
2. Map and maintain cybersecurity control frameworks and regulatory requirements, including National Institute of Standards and Technology (NIST), Center for Internet Security (CIS) Controls, Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS), Payment Card Industry (PCI), and other applicable standards, ensuring alignment with institutional policies and practices.

3. Support the development, review, and maintenance of cybersecurity policies, standards, procedures, and guidelines to ensure compliance with regulatory requirements and industry best practices.
4. Monitor compliance with cybersecurity policies and regulatory obligations, and coordinate audit readiness activities including evidence collection, documentation management, and liaison with internal and external auditors and regulatory entities.
5. Manage cybersecurity exception and risk acceptance processes, including documentation, approval workflows, and periodic review of approved exceptions.
6. Coordinate remediation planning and tracking for audit findings, risk assessments, and compliance reviews, working with system and data owners to ensure timely resolution of identified gaps.
7. Support cybersecurity governance and program initiatives, including compliance assessments, risk reviews, and coordination of mitigation activities across the institution.
8. Develop and maintain cybersecurity metrics, dashboards, and reporting to support operational monitoring, audit readiness, and executive-level decision-making.
9. Lead the development and administration of the University's cybersecurity awareness and training program, including enterprise-wide campaigns, phishing simulations, role-based training, onboarding and annual education, and targeted initiatives to strengthen institutional security culture.
10. Facilitate security engagement efforts as a cybersecurity champions network, outreach activities, and training sessions to promote awareness and shared responsibility across the University system.
11. Prepare reports, briefings, and presentations for executive leadership and governance bodies on cybersecurity risks, compliance posture, and program effectiveness.
12. Leverage artificial intelligence and automation to enhance analysis, reporting, workflow efficiency, and program operations.

Nonessential Duties

- Maintain broad knowledge of emerging cybersecurity governance, regulatory, and compliance requirements.
- Participate in higher education cybersecurity communities and professional groups such as Research and Education Networks Information Sharing and Analysis Center (REN-ISAC), EDUCAUSE, and other similar organizations.

- Support security awareness events, outreach campaigns, and educational initiatives.
- Research emerging regulatory or compliance requirements impacting higher education cybersecurity programs.
- Perform reasonable related duties as assigned.

Supervisory Responsibilities

This position has no direct supervisory responsibilities. This position may provide guidance or coordination for student employees or interns assisting with security awareness or compliance initiatives.

Reporting Relationship

Reports to the Chief Information Security Officer (CISO).

Work Environment

This position operates primarily in a remote work environment and requires the ability to effectively collaborate, coordinate projects, and communicate with distributed teams across the University of Maine System using virtual collaboration tools. Occasional travel to university campuses for meetings, planning sessions, or project coordination may be required. Employees are expected to maintain availability and productivity in remote settings and comply with the University of Maine System's Remote Work Guidelines.

This position has been designated as an "Essential Employee" role. This designation means that, in the event of an emergency (including but not limited to severe weather, natural or human-caused disasters, public health emergencies, operational disruptions, or campus closures), the incumbent is expected to continue work remotely to support ongoing responsibilities.

Knowledge, Skills, and Abilities

Required:

- Knowledge of cybersecurity governance, risk management, and compliance principles
- Knowledge of cybersecurity frameworks and standards including National Institute of Standards and Technology (NIST), Center for Internet Security (CIS)

Controls, International Organization for Standards (ISO) standards, and applicable regulatory requirements
- Knowledge of risk assessment methodologies and security control frameworks
- Knowledge of audit preparation processes and evidence documentation practices
- Ability to analyze cybersecurity risks and develop mitigation recommendations
- Ability to develop policies, procedures, and governance documentation
- Ability to develop reports, dashboards, and metrics for leadership and governance bodies
- Familiarity with artificial intelligence tools and concepts used to support analysis, research, documentation, and workflow efficiency in a professional environment
- Ability to identify opportunities to apply automation or AI-assisted approaches to improve processes, reporting, or operational effectiveness while ensuring appropriate data protection and responsible use
- Strong written communication skills including policy documentation and executive reporting
- Ability to collaborate effectively with technical and nontechnical stakeholders across the University.

Qualifications

Required:

- Bachelor's degree in Cybersecurity, Information Systems, Information Technology, Risk Management, or related field, or an equivalent combination of education and experience
- Five or more years of professional experience in cybersecurity, IT risk management, compliance, or information security program support.
- Demonstrated use of AI-assisted tools or automation to improve security workflows, processes, or reporting.

Preferred:

- Relevant governance, risk, compliance, audit, or privacy certifications such as:
    - CISA - Certified Information System Auditor
    - CRISA - Certified in Risk and Information Systems Control
    - CGRC - Certified in Governance, Risk and Compliance
    - CISM - Certified Information Security Manager
    - CIPP- Certified Information Privacy Professional

    - CIPM - Certified Information Privacy Manager
- Relevant certifications in artificial intelligence, automation, or emerging technologies (e.g., Microsoft AI-900, Google Generative AI Fundamentals, IBM AI Foundations, or similar)
- Experience working in higher education, public sector, or multi-campus organizations.
- Experience supporting cybersecurity governance, risk management, or compliance programs
- Experience coordinating internal or external cybersecurity audits and regulatory assessments
- Experience developing or administering cybersecurity awareness or training programs
- Experience working in higher education or complex enterprise IT environments
- Experience designing, developing, or implementing automation solutions, tools, or applications that improve workflows, reporting, or operational efficiency using artificial intelligence or advanced technologies.

Note: University Services reserves the right to assign reasonably related additional duties and to change or reassign job duties.

Signatures

The signatures indicate the employee and immediate supervisor have reviewed the job description and had the opportunity to edit the document.

Employee: _____ Date: _____

Supervisor: _____ Date: _____