UW HEALTH JOB DESCRIPTION

IS Security Governance, Risk and Compliance Associate Analyst

Job Code: 340033	**FLSA Status: Exempt**	**Mgt. Approval: L. Risberg**	**Date: March 2022**
Department: 1007422 IS - Risk & Compliance		**HR Approval: N. Lazaro**	**Date: March 2022**

JOB SUMMARY

The UW Health IS Security Governance, Risk, and Compliance (GRC) Associate Analysts develop and maintain information security policies and workforce training and awareness. The GRC Associate Analyst serves as a critical resource for staff and leaders regarding information security policy implementation, interpretation, and compliance. The GRC Associate Analyst assesses and prioritizes information security and cybersecurity risk across the organization, facilitates compliance with regulatory requirements and information security policies, and develops and reports on information security metrics.

The GRC Associate Analyst is responsible for reducing information security and cybersecurity risk to UW Health by helping to prioritize and drive remediation efforts throughout the organization through the following:

- Maintaining governance and compliance standards.
- Assisting with risk assessments to identify vulnerabilities internally and within vendor or third-party supplier products.
- Maintaining, communicating, and enforcing information security policies.
- Maintaining risk management strategies, including risk mitigation, risk reduction, risk transfer, the risk exception process and residual risk analysis.

The GRC Associate Analyst executes high-quality, enterprise-class solutions consistent with regulations and established frameworks. The GRC Associate Analyst may work independently or under the direction of more experienced analysts to develop competencies within IS governance, risk and compliance. The GRC Associate Analyst holds team-level responsibilities and works with employees, and leaders across UW Health, the UW School of Medicine and Public Health, and our partners and affiliates.

MAJOR RESPONSIBILITIES

Governance and Compliance

- Implements a data security risk reporting framework, aligned with NIST SP 800-53, for management teams and governance committees.
- Documents technical, administrative, and physical controls to ensure the business demonstrates compliance, ensuring that UW Health meets both the requirements and intent of its regulatory and compliance obligations.
- Facilitates the remediation of control gaps and escalates critical issues to leadership.
- Assists with an exception review and approval process, and assures exceptions are documented and periodically reviewed.
- Prepares for and facilitates examinations by qualified security assessors for regulations such as HIPAA and PCI DSS. Works closely with control owners and internal and external auditors to ensure requests are completed timely.
- Assists with the evaluation of the effectiveness of the information security program by developing, monitoring, gathering, and analyzing information security and compliance metrics for management.

Information Security Risk Assessment

- Documents information security risks and controls based on established risk criteria.
- Assists with security risk assessments of planned and installed information systems to identify vulnerabilities and risks.
- Recommends controls to mitigate security risks identified via risk assessment process.
- Communicates risk findings and recommendations that are clear and actionable by business stakeholders.

Security Policy Management and Workforce Training and Awareness

- Supports workforce security activities including culture, awareness, and training.
- Analyzes information security incidents in collaboration with other stakeholders. Coordinates remediation and awareness training.
- Researches, recommends, and contributes to information security polices, standards, and procedures. Assists with the lifecycle management of information security policies and supporting documents.
- Works with other organizational participants to implement information security policies.

Third-party Supplier and Vendor Risk Management

- Assists with third-party supplier risk assessments to ensure supply chain risk is managed throughout the supplier's lifecycle. Assesses and reports on the risks and benefits for the business as well as mandates for supplier compliance.
- Articulates results of the final assessments to business stakeholders, project sponsors, program managers, and other internal parties.
- Maintains inventory of relevant suppliers/vendors, controls, and risks for ongoing vendor risk management activities.

ALL DUTIES AND REQUIREMENTS MUST BE PERFORMED CONSISTENT WITH THE UW HEALTH PERFORMANCE STANDARDS.

UW HEALTH JOB DESCRIPTION

JOB REQUIREMENTS

Education	Minimum	Associate Degree in Healthcare, Information Technology, Business, or related field (2 years of relevant experience may be considered in lieu of degree in addition to experience below)
	Preferred	Bachelor's degree in Healthcare, Cybersecurity, Information Technology, Engineering, Business, or related field preferred.
Work Experience	Minimum	None
	Preferred	Demonstrated success in a healthcare setting, addressing risk and compliance with regulatory requirements (e.g. PCI DSS, HIPAA, FedRAMP, SOX).
Licenses & Certifications	Minimum	None
	Preferred	Advanced certifications such as HCISSP, CISSP, CEH, CISM, CISA, CCSP, and/or specific training and certification in security risk management and IT controls frameworks, such as NIST CSF and 800-53.
Required Skills, Knowledge, and Abilities		Emerging competency in the following areas: • Leadership including leads with integrity, maintains strategic orientation, demonstrates business & financial acumen, champions innovation, manages execution, leads & develops people • Technical leadership of applicable products or platforms • Leading highly empowered, self-directed teams including cross-functional teams • Communication • Effective team member • Critical thinking • Applying lean management tools • Applying agile methodologies • Mentoring and teaching • Enterprise Security, Privacy, & Info Sharing • Organizational Awareness and Understanding • Technology Awareness and Strategic Planning Other Knowledge, Skills and Abilities • Knowledge of risk assessments, governmental regulations, or implementation of other key GRC functions. • Ability to analyze data and information with an awareness of regulatory requirements that impact the healthcare industry, as well as security frameworks and methodologies. • Ability to work well with people from different disciplines with varying degrees of technical experience. • Attention to detail • Basic problem-solving skills • Ability to work comfortably under pressure and deliver on tight deadlines • Ability to maintain the highest standards of confidentiality, integrity, and personal accountability when working with sensitive and restricted data, including protected health information (PHI)

PHYSICAL REQUIREMENTS

Indicate the appropriate physical requirements of this job in the course of a shift. *Note: reasonable accommodations may be made available for individuals with disabilities to perform the essential functions of this position.*

	Physical Demand Level	**Occasional** Up to 33% of the time	**Frequent** 34%-66% of the time	**Constant** 67%-100% of the time
X	**Sedentary:** Ability to lift up to 10 pounds maximum and occasionally lifting and/or carrying such articles as dockets, ledgers and small tools. Although a sedentary job is defined as one, which involves sitting, a certain amount of walking and standing is often necessary in carrying out job duties. Jobs are sedentary if walking and standing are required only occasionally and other sedentary criteria are met.	**Up to 10#**	**Negligible**	**Negligible**
	Light: Ability to lift up to 20 pounds maximum with frequent lifting and/or carrying of objects weighing up to 10 pounds. Even though the weight lifted may only be a negligible amount,	**Up to 20#**	**Up to 10#** or requires significant walking or standing, or	**Negligible** or constant push/pull of items of negligible weight

	a job is in this category when it requires walking or standing to a significant degree.		requires pushing/pulling of arm/leg controls	
	Medium: Ability to lift up to 50 pounds maximum with frequent lifting/and or carrying objects weighing up to 25 pounds.	**20-50#**	**10-25#**	**Negligible-10#**
	Heavy: Ability to lift up to 100 pounds maximum with frequent lifting and/or carrying objects weighing up to 50 pounds.	**50-100#**	**25-50#**	**10-20#**
	Very Heavy: Ability to lift over 100 pounds with frequent lifting and/or carrying objects weighing over 50 pounds.	**Over 100#**	**Over 50#**	**Over 20#**
List any other physical requirements or bona fide occupational qualifications:				

Work/Environmental: Moderate noise level consistent with an office environment