CAPILANO UNIVERSITY

Classification	Administrator
Original Date:	January 21, 2020
Revision Date:	April 1, 2024 October 27, 2025
Pay Group:	11

MANAGER, SECURITY AUDIT & ASSESSMENT SERVICES

NATURE AND SCOPE OF WORK

Reporting to the Director, DTO and Cybersecurity, Digital Technology Services, (DTS) and a part of the Associate Vice President (AVP) DTS leadership team, the Manager, Security Audit & Assessment Services leads the cybersecurity team that provides security auditing and assessments for digital solutions across the university.

This role will have the opportunity to influence and drive lasting efforts in the University's digital transformation, with significant student and employee impact through the management and monitoring of a robust security audit and assessment program across digital solutions. In close alignment with university wide strategy, critical components of this position include alignment of the security auditing and assessments program with the cybersecurity strategy, risk management framework, vulnerability management program, cybersecurity protection, cybersecurity access controls, cybersecurity detection and incident response plan. The role requires a strong focus on building and maintaining relationships both across the CapU community and externally with sector colleagues and vendors.

KEY RESPONSIBILITIES

- In consultation with the Director, DTO and Cybersecurity plans, implements, and manages the security auditing and assessment program that is guided by developed cybersecurity frameworks, critical security controls and the National Cybersecurity Assessment (NCA) framework.
- Establishes auditing and assessment processes to ensure all digital solutions follow cybersecurity requirements.
- Participates and provides the appropriate level of response to security breaches including incident response.
- Updates auditing and assessment requirements and processes, seeking to consistently improve the program.
- Working with the centralized security services team, identifies and selects appropriate cybersecurity monitoring tools relating to auditing and assessments to ensure no gaps exist in security management across the digital ecosystem.
- Develops patch management schedule to ensure systems are continuously protected.
- Identifies and reports cybersecurity risks through the auditing and assessment program to the Director, DTO and Cybersecurity for appropriate risk management.
- Develops and guides standards upon which security audits are conducted.
- Develops and maintains cybersecurity training material and manages role based specific cybersecurity training, monitors, and reports compliance to cybersecurity training across the university community

- Conducts audits to ensure that cybersecurity training compliance is at an adequate level at the university.
- Performs follow up with university community members who are not compliant, including managing the refresher program.
- Reports and represents cybersecurity related incidents and risks to the audit and risk committee and at the board level.
- Develops and updates security assessment requirements to develop security threat risk assessment (STRA) reports.
- Manages and continuously follows up on any risks identified and documented in STRA reports to ensure they are mitigated and resolved.
- Analyzes, investigates, and evaluates emerging cybersecurity technology and software trends, including product road maps, to determine impact on DTS roadmap.
- Builds working relationships and partnerships across the university community and sector, providing expert advice on committees, initiatives and engaging with external communities of practice.
- Manages vendor relationships, including development of RFPs, evaluation of proposals, and management of vendor performance, support agreements and licensing.
- Contributes to team development through engaged mentorship and knowledge sharing to help team members grow their cybersecurity experience and skills.

KEY COMPETENCIES

- Job knowledge: knowledge and experience with cybersecurity best practices; demonstrates proven leadership experience in developing strategies, plans, programs and policies related to the delivery of cybersecurity strategy and operations.
- Service focus: understands the role of cybersecurity and digital solutions, and how change affects teams and processes; delivers services that align with the DTS roadmap that support the university's key priorities of exceptional student and employee experience.
- Result oriented: feels personally committed and accountable to deliver results quickly, accurately, and effectively; uses thoughtful judgement when responding to situations that are not going well and uses foresight to overcome obstacles.
- Initiating action / taking initiative: embraces a continuous improvement mindset in an ongoing effort to improve services and processes; readily acts consistent within departmental or university objectives; volunteers readily and takes independent actions when appropriate.
- Leadership and supervisory abilities: encourage and supports cross-functional, high-performing teams; attracts and selects the best talent; coaches and inspires people; sets expectations, recognizes achievement, and proactively manages conflict.
- Problem solving and decision-making: ability to understand complex systems and processes and find diverse solutions to stubborn problems; makes clear, consistent, and transparent decisions; acts with integrity in all decision making.
- Strategic planning and organizing: Demonstrated capacity to develop and implement strategies,

tactical plans, policies, and procedures. Experience managing a cybersecurity program.

- Employee development: achieve desired organizational results by encouraging and supporting the contribution of others; modeling positive leadership behaviours, including integrity, honesty, a sense of urgency and leading by example.

EDUCATION / TRAINING AND EXPERIENCE

- 5+ years of relevant professional experience, with 1 years in a recent leadership role with direct responsibility for a cybersecurity program, preferably in a public sector environment.
- Demonstrated experience in leading a cybersecurity program.
- Demonstrated experience in conducing audits, assessments and writing STRA reports.
- A bachelor's degree
- Industry relevant designations such as CISSP, CISA, CRISC, ITIL, TOGAF.
- Experience with the ITIL framework and ITSM best practices, tools, and techniques; ITIL certification is an asset.
- Demonstrated knowledge of vulnerability and patch management, security auditing and assessment of cloud solutions, and privacy.
- Broad technical knowledge relating to cybersecurity practices, including patching, firewalls, network configurations, phishing, and software deployment.
- Demonstrated experience in effectively communicating and presenting cybersecurity audits and assessments to varies levels within an organization.
- Demonstrated experience in developing STRA reports and reviewing these with a mix of technical and management positions.
- Completion of a criminal record check.