

Position Description

PROFESSIONAL SERVICES

Position Title	Senior Business Analyst - Cyber
Classification/Level under the Enterprise Agreement (if applicable)	Level 8-9 (Fixed Term)
Management Level	Specialist / Administration / Support
Faculty / Portfolio	Operations
School / Division	Information Management & Technology Services
Main Location(s)	Wollongong Campus (2 days per week)
Delegations (if applicable)	This position may carry delegations in accordance with the UOW Delegations of Authority as amended from time to time.

Primary Purpose of the Position

The Senior Business Analyst will play a critical role in supporting the effective design and implementation of cyber security initiatives. The position will work closely with vendors, project managers, business stakeholders, and technical staff throughout the design and implementation lifecycle to deliver new cyber security controls, uplifting existing controls and processes, and ensure alignment with UOW's digital strategy to uplift cybersecurity maturity.

It includes coordination of project day to day activities, problem identification and scoping, organising and facilitating workshops, As-Is and To-Be process mapping, gathering technical and business requirements, ensuring testing is effective and validation of requirements, etc.

The role will also contribute to maintaining accurate records and plans for the project, providing project activity coordination e.g., organising and facilitating workshops, and assist in identifying new opportunities for process improvement.

Additionally, this role will analyse and examine new ideas and initiatives relating to the improvement of business processes and assist the creation and execution of associated cyber security projects.

Position Environment

Information Management & Technology Services (IMTS) is the University's central information management and technology service provider for core infrastructure and services and is responsible for the development and management of information and communications technology resources in response to research, teaching and corporate requirements.

This position reports to the Cyber Security Program Director and works closely with functional managers, portfolio managers, business unit leaders, technical experts and project delivery teams.

Major Responsibilities

- Stakeholder Engagement & Facilitation:**
 - Responsibility: Facilitate workshops and engage stakeholders across business, ICT, and cyber teams
 - Objective: Ensure alignment, shared understanding, and agreement on cyber security outcomes
- Requirements Elicitation & Management:**
 - Responsibility: Gather, analyse, and document business and technical requirements.
 - Objective: Ensure clear, complete, and traceable requirements that meet business and security needs.
- Business & Process Analysis:**
 - Responsibility: Conduct current/future state analysis, gap analysis, and process mapping
 - Objective: Identify control gaps and design improved processes aligned to frameworks like National Institute of Standards (NIST)
- Solution Design Support:**
 - Responsibility: Support solution design in collaboration with architects, SMEs, and vendors.
 - Objective: Ensure solutions are fit-for-purpose and aligned to business requirements and security controls.
- Testing, Validation & Assurance:**
 - Responsibility: Support test planning, execution, and validation of solutions
 - Objective: Confirm delivered solutions meet requirements and are fit for use.



6. **Cyber Security Activities & Assurance:**
 - Responsibility: Participate in and document penetration testing and security assessments.
 - Objective: Translate technical findings into business risks and actionable remediation.
7. **Project Delivery & Coordination:**
 - Responsibility: Contribute to project planning, coordination, and delivery activities.
 - Objective: Support timely delivery and alignment across project workstreams.
8. **Continuous Improvement & Documentation:**
 - Responsibility: Support process improvement and development of SOPs and ISMS artefacts.
 - Objective: Drive consistency and uplift in cyber security capability and practices.
9. **Stakeholder & Vendor Management:**
 - Responsibility: Collaborate with internal teams and external vendors/partners.
 - Objective: Ensure effective delivery and integration of third-party solutions
10. Act in accordance with University policies as amended from time to time, the Values in Action Framework of *Thrive Together, Pursue Excellence, Be Accountable and Lead with Integrity*, and our commitment to Equity, Diversity and Inclusion.
11. WHS responsibilities, accountabilities and authorities as outlined in the WHS Framework - <https://www.uow.edu.au/about/services/safe-at-work/whs-framework/>

Reporting Relationships and Other Key Contacts

Position reports to	Associate Director of Security (CISO) via the Cyber Security Program Director.
Positions supervised by this position	This role will not supervise any positions but will take on a directing role for program resources including, Business Analysts, Security Analysts, Solution Architects, Change Managers, etc., as well as IMTS and business subject matter experts to ensure that strategic goals are met.
Other key contacts and stakeholders	• Chief Information and Digital Officer, IMTS • Cyber Security Uplift Program - Program and project resources. • IMTS Senior Management Team: • Associate Director, Infrastructure & Communication • Associate Director, Client Products & Services • Associate Director, Global & Controlled Entities • Associate Director, Development Services • Head of Digital Strategy & Architecture • IMTS – Cyber Security Ops, Infrastructure, enterprise architecture, and client services teams. • UOW community - UOW system owners, academic facility providers and other UOW key IT stakeholders. • External - Third party vendors and other security suppliers.

Selection Criteria

Essential:

- Minimum of 5 years' experience in a senior business analyst role on Cyber projects implementing technical security solutions
- Strong background in requirements development, business process re-engineering, and business systems specification
- Experience with project management, testing, QA, and system deployment methodologies
- Strong team player with the ability to collaborate effectively across a diverse project team and technical SME's
- Proven ability to work with both business and technical stakeholders, including managing challenging stakeholder relationships
- Experience working with vendors and external partners
- Tertiary qualification in Business, IT, or a related discipline (or equivalent experience/training)



Desirable:

- Knowledge of cyber security technologies and cyber security frameworks such as ISO 27001, NIST CSF, or Essential Eight.
- Experience within the Australian higher education sector
- Relevant business analysis certification (e.g., Certified Business Analysis Professional (CBAP), Certified ScrumMaster (CSM), etc).
- Relevant security certifications (e.g., CISSP, CISM, SABSA, or equivalent) or strong understanding of enterprise security practices.

Special Job Requirements

- May be required to work outside of standard business hours or across campuses and research partner facilities.
- This position is subject to a National Criminal Check.
- Maybe be requirement to work outside of standard business hours.
- Restriction on leave during peak periods may apply.

Roles and Responsibilities in relation to Workplace Health and Safety and Equity, Diversity and Inclusion in the Workplace

The University of Wollongong is committed to providing a safe, inclusive, and equitable workplace for its workers, students and visitors. All members of the University community have a collective and individual responsibility to work safely, be engaged in activities to help prevent injuries and illness and create an equitable and inclusive environment.

In addition to the major accountabilities/responsibilities required for your position, you also hold the following roles and responsibilities in relation to Workplace Health and Safety:

ALL STAFF

- Take reasonable care for your health and safety as well as others.
- Comply with any reasonable instruction by the University.
- Cooperate with any reasonable policies and procedures of the University including reporting of hazards or incidents via the University reporting process.
- Certain staff have specific responsibilities for Work Health and Safety (WHS), further information is available in the [WHS Framework](#).
- Work in an inclusive environment, treating all colleagues, students and visitors with respect.

ADDITIONAL RESPONSIBILITIES FOR STAFF WITH SUPERVISORY RESPONSIBILITIES

- Uphold principles of equity, diversity and inclusion and foster a respectful workplace culture within your team.
- Ensure work area, equipment and practices are compliant with applicable legislation, standards, codes of practice and University guidelines.
- Ensure risk management activities are undertaken to minimise WHS risk including hazard and incident reporting, risk assessment and safe work procedures.
- Provide the necessary instruction, information, induction, training and supervision to enable work to be carried out safely.
- Ensure Work Health and Safety (WHS) activities and requirements are implemented for area as outlined in the WHS Framework.

Inherent Requirements

This position description outlines the major accountabilities/responsibilities and the selection criteria against which you will be assessed as suitable for the position. As such there will be specific job requirements that we refer to as Inherent Requirements.

Inherent Requirements refer to your ability to:

- Perform the essential duties and functional requirements of the job;
- Meet the productivity and quality requirements of the position;
- Work effectively in the team or other relevant work organisation; and
- Do the job without undue risk to your own or others health, safety and wellbeing at work.

If you have any injuries, illness, disorder, impairment, condition, disability or incapacity that may affect your ability to perform the inherent requirements of the position, we encourage you to discuss this with the University to assist in the process of identifying reasonable adjustments to enable you to perform the duties of the position. The University wants to place you in the best situation to use your skills effectively in the position you are applying for at the University.



Position Description Status

This table contains information about the status and approval of this document

Date created	2 Sep 2026
Date reviewed by supervisor in consultation with the employee i.e. at least every three (3) years, or sooner if required	
Date reviewed by P&C (if applicable)	
Date reviewed by CP&CO (if applicable)	
Date of next review	

