Qualification details

Title	New Zealand Diploma in Cybersecurity (Level 6)		
Version	1	**Qualification type**	**Diploma**
Level	6	**Credits**	**120**
NZSCED	029901 Information Technology > Other Information Technology > Security Science		
Qualification developer	NZQA National Qualifications Services (NQS)		
Next review	31 October 2023		
Approval date	October 2018		
Strategic purpose statement	*This qualification was co-developed by IT Professionals New Zealand (ITP) and NZQA National Qualifications Services (NQS).* The purpose of this qualification is to provide Aotearoa New Zealand with people who have attained internationally transferable industry-relevant knowledge and technical skills that will equip them to work in entry-level roles in the specialised field of cybersecurity, or to proceed to further study. Businesses, organisations and communities will benefit from having cybersecurity professionals who have developed a security mindset and who are able to identify, mitigate and respond to cybersecurity risks and incidents, and help assure information and systems security, integrity and availability. Graduates will be capable of operating within the applicable professional standards and practice, both independently and as part of a team.		
Outcome Statement	**Graduate profile**	Graduates of this qualification will be able to: *Technical skills* 1. Analyse organisational contexts from a security perspective using information management principles and terminology, data inputs, organisational strategy and processes, outputs, systems, and stakeholders' roles and responsibilities. 2. Analyse an IT environment's technology stack from a security perspective and identify issues that could impact organisational performance and business risks. 3. Apply knowledge of risk management frameworks to perform cybersecurity risk assessments and communicate the results to support the organisational risk management process. 4. Assess, select, plan, implement and validate cybersecurity approaches and controls to support organisational objectives and operations. 5. Analyse cybersecurity events, perform security incident		

		classification, and apply relevant security incident handling techniques, whilst participating in an incident handling process. 6. Analyse the legal, privacy and ethical impacts of the regulatory environment, and organisational decisions to advise decision makers on cybersecurity implications and organisational obligations applicable to a particular situation. *Core skills* 7. Behave with integrity as a responsible IT professional, in accordance with legal and organisational regulatory requirements, applying professional and ethical practices. 8. Apply communication, information design, teamwork, personal, and interpersonal skills, to enhance working effectiveness, efficiency, and quality outcomes in a variety of situations in an organisational environment. 9. Apply project management tools and techniques, using knowledge of project planning, management and control, to an IT related project, to analyse and solve problems.
	Education pathway	This qualification provides an education pathway from: • New Zealand Diploma in Information Technology Technical Support (Level 5) [Ref: 2596] • New Zealand Diploma in Information Systems (Level 5) [Ref: 2597] • New Zealand Diploma in Web Design and Development (Level 5) [Ref: 2598] • New Zealand Diploma in Software Development (Level 6) [Ref: 2604] or other Level 5 IT-related qualifications; or relevant industry experience, to specialised re-training into the field of cybersecurity. This qualification provides a pathway to further specialisation through industry-specific training in specialist fields of cybersecurity, and industry certifications. Other education pathways include higher level IT-related qualifications and industry certifications.
	Employment pathway	Graduates of this qualification will have the skills and knowledge to gain employment in entry-level roles in the specialised field of cybersecurity such as security analyst, security tester, security administrator, incident analyst, information assurance analyst, security assessor/auditor, security engineer, security developer or other cybersecurity related support roles. Graduates will also have the skills and knowledge to progress into more advanced roles including cybersecurity analyst, engineer or manager.

Qualification specifications

Qualification award	This qualification may be awarded by any education organisation with an approved programme of study or industry training.
Evidence requirements for assuring consistency	Evidence requirements may include: - effective internal and external moderation systems and processes, including results relating to graduate outcomes; - results of end-user surveys and actions taken or proposed from feedback. This includes consultation with graduates and employers to obtain destination information and end-user feedback specifically assessing the graduates against the graduate profile (e.g. employment, progression, further study); - samples of assessment materials and learners assessments/work (e.g. portfolios of work); - evidence of any benchmarking activities.
Minimum standard of achievement and standards for grade endorsements	The minimum standard of achievement required for the award of the qualification will be the achievement of all the graduate outcomes. There are no grade endorsements for this qualification.
Other requirements for the qualification (including regulatory body or legislative requirements)	Current legislation and regulations can be accessed at www.legislation.govt.nz Current AS/NZS standards can be accessed at www.standards.govt.nz Relevant codes of ethics and professional practice, including the following, which can be accessed at: - ITP Code of Ethics: www.itp.nz/Members/Code-of-Ethics - ITP Professional Practice Guidelines, including the ITP Code of Practice and ITP Professional Knowledge Curriculum: www.itp.nz/Members/Practice-Guidelines Computer Emergency Response Team (CERT NZ) provides up-to-date, actionable advice on current threats and vulnerabilities, as well as guidance on mitigation and cyber security best practice, available at www.cert.govt.nz/it-specialists.

General conditions for the programme leading to the qualification

General conditions for programme	***Programme entry*** It is recommended that people enrolling on programmes hold one of the following: • New Zealand Diploma in Information Technology Technical Support (Level 5) [Ref: 2596] • New Zealand Diploma in Information Systems (Level 5) [Ref: 2597] • New Zealand Diploma in Web Design and Development (Level 5) [Ref: 2598] • New Zealand Diploma in Software Development (Level 6) [Ref: 2604] • first year of an IT degree and/or equivalent knowledge, skills and experience.

	Programme design Programmes should integrate the assessment of core skills (outcomes 7-9) with the technical skills (outcomes 1-6). Programmes must reflect quality industry practice and maintain currency with amendments to, and replacements of, relevant legislation, regulations, Australia/New Zealand standards (AS/NZS), and security responsibilities including cyber safety. Programmes must reflect relevant codes of ethics and professional practice. Programmes must include the role of regulators/Governments, and identifying the implications of laws, regulations, and international treaties applicable to a particular situation. Programmes may be developed based on Māori principles and values and they may enable Wānanga to meet obligations under the Education Act (1989, section 162(4)(b)(iv)). ***Diversity*** To encourage greater diversity within the professional IT workforce, consideration should be given to bicultural, multicultural, and gender issues when designing programmes. ***Professional practice*** Professional practice must be an integral part of the programme and delivery. Professional practice includes the core 'soft skills' of communication, team work, interpersonal skills, and ethical principles and practices. It also includes the organisational implications of managing and complying with legal and regulatory requirements (e.g. health and safety, contract management, licensing, privacy); observing security responsibilities and industry codes of practices, and codes of conduct, relevant to an organisational environment. ***Practical experience*** Practical experience is essential, and it is recommended that programmes include learners completing at least half of the study in real or realistic practical settings. A real or realistic practical setting may include workplaces, labs or other simulated environments, or table-top walk through exercises.

Conditions relating to the Graduate profile

Qualification outcomes		Conditions
	Technical Skills	
1	Analyse organisational contexts from a security perspective using information management principles and terminology, data inputs, organisational strategy and processes, outputs, systems,	Programmes must include classifying organisational assets and sensitivity of data.

	and stakeholders' roles and responsibilities. Credits 10	
2	Analyse an IT environment's technology stack from a security perspective and identify issues that could impact organisational performance and business risks. Credits 15	Programmes must include enterprise and systems interdependencies and the potential vulnerabilities and weaknesses of current and emerging technologies and architectures.
3	Apply knowledge of risk management frameworks to perform cybersecurity risk assessments and communicate the results to support the organisational risk management process. Credits 20	Programmes must include understanding and communication of risk appetite and cost/benefit trade-offs.
4	Assess, select, plan, implement and validate cybersecurity approaches and controls to support organisational objectives and operations. Credits 25	Programmes must include security by design concepts and secure development techniques; the interdependence of cybersecurity with technical and physical controls, and human factors, including the relationship with usability.
5	Analyse cybersecurity events, perform security incident classification, and apply relevant security incident handling techniques, whilst participating in an incident handling process. Credits 15	Programmes must include identification of the information needed for security incident classification.
6	Analyse the legal, privacy and ethical impacts of the regulatory environment and organisational decisions, to advise decision makers on cybersecurity implications and organisational obligations applicable to a particular situation. Credits 5	Programmes must include risks and opportunities around legally grey areas such as unauthorised testing, exploit marketplaces, and vulnerability disclosure.
	Core Skills	
7	Behave with integrity as a responsible IT professional, in accordance with legal and organisational regulatory requirements, applying	

	professional and ethical practices. Credits 10	
8	Apply communication, information design, teamwork, personal, and interpersonal skills, to enhance working effectiveness, efficiency, and quality outcomes in a variety of situations in an organisational environment. Credits 10	Programmes must include information representation design for a variety of situations such as data visualisation; technical writing - help documents, user instructions, specifications.
9	Apply project management tools and techniques, using knowledge of project planning, management and control, to an IT related project, to analyse and solve problems. Credits 10	Programmes must include critical thinking, business logic, organisational processes, innovation and enterprise skills.