Title	**Produce security risk assessments**		
Level	**6**	**Credits**	**20**

Purpose	This unit standard is for people who work, or intend to work, as security managers or security consultants, and who need to produce security risk assessments. People credited with unit standard are able to: - establish the context for the security risk assessment; - identify security risks; - analyse security risks; - evaluate and prioritise security risks; and - document and present security risk assessment.

Classification	Security > Security Management

Available grade	Achieved

Guidance Information

1 References
Aviation Crimes Act 1972;
AS/NZS 31000:2009 *Risk Management - Principles and guidelines,* available from https://www.standards.govt.nz/;
Building Act 2004;
Biosecurity Act 1993;
Civil Defence Emergency Management Act 2002;
Crimes Act 1961;
Employment Relations Act 2000;
Evidence Act 2006;
Fire and Emergency New Zealand Act 2017;
Good Practice Guidelines, New Zealand Security Association, available from https//www.security.org.nz/;
HB 167: 2006 *Security risk management,* available from https://www.standards.govt.nz/;
Health and Safety at Work Act 2015;
Human Rights Act 1993;
Intelligence and Security Act 2017;
ISO 31000:2018 *Risk management guidelines,* available from https://www.standards.govt.nz/;
Maritime Security Act 2004;
Maritime Security Regulations 2004;
New Zealand Bill of Rights Act 1990;
Official Information Act 1982;
Oranga Tamariki Act 1989;

Policing Act 2008;
Privacy Act 2020;
Private Security Personnel and Private Investigators Act 2010;
Resource Management Act 1991;
Sale and Supply of Alcohol Act 2012;
Search and Surveillance Act 2012;
Secret Commissions Act 1910;
Summary Offences Act 1981;
Terrorism Suppression Act 2002;
Trespass Act 1980;
and all subsequent replacements and amendments.

2 Definitions

Analysis – the systematic examination and organisation of information.
Assessment – the analysis and evaluation of data to establish facts, value, and credibility.
Best practice – an industry approved current method or way of doing something that, in the circumstances, achieves the required outcome.
Client – the person(s), or entity who contracts the task.
Evaluation – the examination and comparison of information against accepted or required standards and/or other criteria to determine its value and relevance.
Organisation – a company, firm, enterprise or association, or other legal entity or part thereof, whether incorporated or not, public or private, that has its own function(s) and administration.
Organisational policy and procedures – instructions to staff on policies, procedures, and methodologies which are documented and are available in the workplace.
Risk – the chance of something happening that will have an impact upon objectives, measured in terms of consequences and likelihood.
Risk assessment – the overall process of risk analysis and risk evaluation.
Risk evaluation – the process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels, or other criteria.
Risk management – the systematic application of policy, practice and procedure to the task of identifying, analysing, assessing, treating and monitoring risk.
Security – the protection of people, activities, and assets including information, from loss, damage, or harm.
Security investigation – a planned and directed process used to establish facts relevant to security.
Security measures – *strategies*, systems and resources used to ensure security.

3 Assessment Range

Evidence of two fully documented risk assessments is required.

Outcomes and performance criteria

Outcome 1

Establish the context for the security risk assessment.

Performance criteria

1.1 Identify the strategic environment in which the organisation operates and identify key stakeholders in accordance with organisational policy and procedures.

1.2 Identify the organisational capabilities, goals and objectives, and identify the strategies used to achieve them.

1.3 Identify the scope and boundaries for the risk assessment in accordance with organisational policy and procedures.

Range scope and boundaries – objectives, time, resources, special studies, extent and comprehensiveness, relationship to other projects.

1.4 Specify the criteria against which the security risks are to be evaluated in accordance with best practice.

1.5 Define a logical framework to facilitate subsequent identification and analysis of security risks in accordance with best practice.

1.6 Identify key contacts in the organisation for the purpose of the risk assessment.

Outcome 2

Identify security risks.

Performance criteria

2.1 Identify security risks with a comprehensive list of events and potential threats relevant to the risk assessment.

2.2 Identify security risks with possible causes and scenarios for each of the identified security events.

2.3 Identify security risks using relevant tools and techniques.

Range typical tools and techniques may include but are not limited to – checklists, records of past events, flow charts, system analysis, scenario analysis, interviews, consultation, past surveys and assessments, security investigations.

Outcome 3

Analyse security risks.

Performance criteria

3.1 Analyse security risks to identify and evaluate existing security measures in accordance with best practice.

Range security measures – management, technical systems, procedures.

3.2 Analyse security risks to establish the likelihood of occurrence, and the consequences of each event in the context of the identified measures.

3.3 Combine consequences and likelihood in the analysis to produce a level of risk in accordance with best practice.

Range analysis may involve but are not limited to calculations and statistical analysis, and/or subjective estimates reflecting the belief that particular events or outcomes may occur.

3.4 Analyse security risks to consider the effect of changes in assumptions and data.

Outcome 4

Evaluate and prioritise security risks.

Performance criteria

4.1 Evaluate and prioritise security risks in accordance with pre-established evaluation criteria and, where appropriate, identify low risk categories requiring no further treatment.

Outcome 5

Document and present security risk assessment.

Performance criteria

5.1 Document and present security risk assessment, appropriate to the nature of the risk assessment and meet client expectations.

Range documentation and presentation must include – evidence of care in presentation; substance, credibility, and clarity are not compromised by deficient spelling, punctuation or grammar; the meaning of technical terms is clear to recipients or is explained; client expectations may include – timeliness, content, clarity, conciseness, complexity, level, medium.

5.2 Document and present security risk assessment to meet professional standards.

Range standards must include – content is structured in a logical and coherent sequence;
there are no substantive omissions or errors of fact;
assumptions, comment, inferences, conclusions and recommendations are distinguished from fact;
conclusions and recommendations are unbiased;
conclusions and recommendations are consistent with the brief or objectives, facts, analysis, and evaluation;
relevant legal and regulatory requirements are satisfied.

5.3 Secure documentation and presentation consistent with content and client needs.

Planned review date	31 December 2025

Status information and last date for assessment for superseded versions

Process	Version	Date	Last Date for Assessment
Registration	1	21 March 2003	31 December 2023
Review	2	28 January 2021	N/A

Consent and Moderation Requirements (CMR) reference	0003

This CMR can be accessed at http://www.nzqa.govt.nz/framework/search/index.do.

Comments on this unit standard

Please contact The Skills Organisation reviewcomments@skills.org.nz if you wish to suggest changes to the content of this unit standard.