Title	**Apply security techniques, hardware, and systems to minimise risk**		
Level	**6**	**Credits**	**25**

Purpose	This unit standard is for people who apply, or intend to apply, security techniques, hardware and systems to minimise risk. People credited with this unit standard are able to: - describe and assess security techniques to minimise risk; - describe security hardware and systems to minimise risk; and - apply security techniques, hardware, and systems to minimise risk.

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 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.
Risk – the chance of something happening that will have an impact upon objectives, measured in terms of consequences and likelihood.
Risk analysis – the systematic use of available information to determine how often specified events may occur and the magnitude of their impact on the organisation.
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 survey – an activity to establish facts relevant to security for a specific environment.

Outcomes and performance criteria

Outcome 1

Describe and assess security techniques to minimise risk.

Range security techniques – risk analysis, deterrence, access control, information control, personnel vetting, crowd control, surveillance, security investigation, disaster recovery, system integration, training, environmental design, security survey.

Performance criteria

1.1 Describe security techniques in terms of their purpose, methods, benefits, and costs in accordance with best practice.

1.2 Assess the application of security techniques in given risk situations in terms of effectiveness and resource management.

Range assessment to cover five different security techniques across three of the following risk situations – industrial, domestic, commercial, public.

Outcome 2

Describe security hardware and systems to minimise risk.

Performance criteria

2.1 Describe security hardware items with reference to features, capabilities, limitations, and costs.

Range evidence of five security hardware items is required.

2.2 Describe electronic security devices with reference to features, capabilities, limitations, and cost.

Range evidence of five electronic security devices is required.

2.3 Describe electronic security systems with reference to features, capabilities, limitations, and cost.

Range evidence of five electronic security systems is required.

Outcome 3

Apply security techniques, hardware, and systems to minimise risk.

Range two applications are required – of these, at least one must be from:
commercial – bank, office building, supermarket, shopping mall, telecommunications facility; or
industrial – factory, power station, storage facility; or
transport – airport, rail terminal, port, marina; or
public – parliament, museum, venues, educational facility.

Performance criteria

3.1 Specify security techniques, hardware, and systems appropriate to the risk situation and application.

Range specification of security items must indicate type, size, and/or quantity, but need not refer to specific brands, models, or ratings.

3.2 Detail specified security items in a schedule and indicate their locations on a plan to enable specialists to prepare quotations and installation plans.

3.3 Justify the selection of each specified security item with reference to need, performance, and cost.

Replacement information	This unit standard replaced unit standard 15285.

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.