Title	**Apply security principles, practice, and procedure to resolve and provide advice on security issues**		
Level	**6**	**Credits**	**15**

Purpose	This unit standard is for people who work, or intend to work, as security managers or security consultants, and who need to apply security principles, practice, and procedure to resolve and provide information and advice on security issues. People credited with this unit standard are able to: - demonstrate knowledge of security principles, practice, and procedure; - resolve security issues using security principles, practice, and procedure; and - provide information and advice on security issues.

Classification	Security > Security Management

Available grade	Achieved

Guidance Information

1 Resources
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.

Assets – in terms of security, assets are people and their activities, physical and intellectual property, information, and functions, processes and systems.

Best practice – an industry approved current method or way of doing something that, in the circumstances, achieves the required outcome.

Common security risks – risks common to most sites including but not limited to: trespass and unauthorised access; unsafe, disorderly, or disruptive behaviour; deliberate damage and destruction; other crime including theft, burglary, robbery and assault; safety and security breaches and incidents; emergencies or critical incidents resulting from fire, structural damage or failure, accidents, critical medical conditions, natural disasters including storms and earthquakes, flooding, leaks and spills of hazardous substances, and process and system failures, loss or compromise of information.

Evaluation – the examination and comparison of information against accepted or required standards and/or other criteria to determine its value and relevance.

Organisational policy and procedures – instructions to staff on policies, procedures, and methodologies which are documented and are available in the workplace.

Physical risk – risk from physical threats to people, activities, and assets including crime, other inimical activities, natural events, and fire.

Protective security – the systematic application of resources, systems and other measures to protect people, property, information and other assets, and activities, from physical risk.

Security – the protection of people, activities, and assets including information, from loss, damage, or harm.

Security issues – issues relevant to security and security practitioners/managers and consultants including but not limited to common security risks, staff recruitment and employment; security events, incidents and breaches; complaints; information loss or compromise; employee theft or fraud; security policy, practice and procedure; misuse of drugs and or alcohol; misuse of property; staff and customer access; fire safety; security systems and equipment; personal safety.

Security practice – strategies, actions and measures implemented to ensure security and accepted by industry as best practice.

Security principles – the general precepts on which security relies and which underpin best practice. Security principles include: *cost* - the cost of any security measures relates to or is proportional to assessed security risk and benefits; *depth* - provides multi-layer protection or sequential barriers; *mutual support* - each security measure is supported and or protected by another; *need to know* - information about security matters is restricted to those who must know; *compatibility* - measures reflect operational and environmental conditions, and necessity, and are not unduly restrictive; *reliability* - reliability is ensured, potential and actual failures are signalled and result in a safe condition, systems should be failsafe.

Outcomes and performance criteria

Outcome 1

Demonstrate knowledge of security principles, practice, and procedure.

Range sectors may include but are not limited to – primary industry, manufacturing and processing, commercial services, financial, corporate, entertainment, hospitality, transport, communications, paramedical and medical, government, and domestic sectors of society and the economy.

Performance criteria

1.1 Describe the purpose, scope, and objectives of security in accordance with best practice.

Range must provide two examples in each of three different sectors.

1.2 Explain the principles on which protective security relies in accordance with best practice.

Range must provide two examples in each of three different sectors.

1.3 Describe common security risks in terms of their nature, relevance, and impact in accordance with best practice.

Range must provide one example in each of three different sectors.

1.4 Describe security practice and procedure in terms of their nature, application, and effectiveness with reference to workplace examples.

Range must provide one example in each of three different sectors.

1.5 Explain security functions, resources, and structure in terms of the products and services they provide with reference to workplace examples.

Range must provide one example in each of three different sectors.

Outcome 2

Resolve security issues using security principles, practice, and procedure.

Range issues must include – two common security risks and two other security issues from the definition of security issues.

Performance criteria

2.1 Identify and assess security issues in terms of their nature, cause, and impact in accordance with best practice.

2.2 Resolve security issues using immediate responses consistent with relevant law and compliance guidelines including policy and procedure, and prioritise in accordance with relevant factors.

Range typical immediate responses must include – informing others, obtaining further information, damage control, liaison and co-operation, obtaining advice and support, obtaining technical or specialist support, ensuring safety.

2.3 Resolve identified security issues by stating and implementing recommendations, strategies, and actions in accordance with best practice, and organisational policy and procedures.

Outcome 3

Provide information and advice on security issues.

Range issues must include – two common security risks and two other security issues from the definition of security issues;
issues relate to a specific entity or activity, or to a series of identified entities or activities.

Performance criteria

3.1 Provide information and advice to the recipient according to their needs.

Range needs must include – fit for purpose, scope, sufficiency, timeliness, structure and format, communication method, clarity, security, privacy.

3.2 Ensure credibility of the information or advice by reference to the process used to produce it.

Range processes must include – analysis, evaluation, best practice model, influencing factors, assumptions.

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.