Title	**Develop operational security plans**		
Level	**6**	**Credits**	**20**

Purpose	This unit standard is for people who develop, or intend to develop, operational security plans. People credited with this unit standard are able to: - establish operational security objectives; - identify and assess operational parameters for an operational security plan; - formulate and deliver operational security plans; and - document and present operational security plans.

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.
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.
Operational security plan – a statement of strategies, actions and measures to achieve a desired outcome.
Procedure – a way of acting or progressing, especially an established method.
Relevant instructions – oral, written or electronically transmitted instructions issued to govern the performance of security tasks, duties, and responsibilities. These may be in the form of policies, procedures, manuals, directives, or legal and compliance requirements. They may relate to a particular assignment, organisation, site or operation of equipment.
Risk – the chance of something happening that will have an impact upon objectives, measured in terms of consequences and likelihood.
Security – the protection of people, activities, and assets including information, from loss, damage, or harm.
Target – in terms of security, targets are people and their activities, physical and intellectual property, information, and functions, processes and systems that are the focus of inimical interest.

3 Assessment Range
This standard must be assessed using best practice for actual situations.
Evidence of two fully documented operational security plans is required.

Outcomes and performance criteria

Outcome 1

Establish operational security objectives.

Performance criteria

1.1 Establish objectives for an operational security plan consistent with the strategic intent of the organisation and/or client.

1.2 Demonstrate objectives for an operational security plan in measurable terms in accordance with best practice.

Outcome 2

Identify and assess operational parameters for an operational security plan.

Range specific areas may include –
infrastructure; personnel – skills, knowledge, availability, training, number, location; equipment – capability, availability, reliability, contingencies; finance - cost benefit analysis;
time – milestones, timelines, holidays; environment - legislation, regulations, standards, culture;
commercial – contracts, market situation.

Performance criteria

2.1 Identify operational parameters likely to influence operational objectives in accordance with relevant instructions.

2.2 Assess operational parameters in terms of their influence on the achievement of the operational objectives.

Outcome 3

Formulate and deliver operational security plans.

Performance criteria

3.1 Formulate operational security plan to include the application and integration of relevant security concepts, techniques and technology in accordance with best practice.

3.2 Formulate the operational security plan to include personnel requirements, responsibilities, and performance targets in accordance with best practice.

3.3 Formulate the operational security plan to include equipment requirements and performance targets in accordance with best practice.

3.4 Formulate the operational security plan to meet identified financial constraints in accordance with best practice.

3.5 Formulate the operational security plan to specify and assess operational risks and costs in accordance with best practice.

3.6 Formulate the operational security plan to include timelines, milestones, and critical dates and/or times in accordance with best practice.

3.7 Formulate the operational security plan to make specific provisions for implementation procedures, contingency plans, coordination, monitoring, and improvement processes in accordance with best practice.

3.8 Deliver operational security plan within agreed timeframes in consultation with stakeholders in accordance with best practice.

3.9 Formulate the operational security plan to comply with legislative and regulatory requirements.

Outcome 4

Document and present operational security plans.

Performance criteria

4.1 Document and present operational security plan, appropriate to the nature of the plan and meet client expectations.

Range documentation and presentation – 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 but are not limited to – timeliness, content, clarity, conciseness, complexity, level, medium.

4.2 Document and present operational security plan to meet professional standards.

Range standards may 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.

4.3 Secure the documentation and presentation is consistent with its 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	30 September 1998	31 December 2023
Revision	2	3 April 2001	31 December 2023
Review	3	21 March 2003	31 December 2023
Review	4	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.