Title	**Conduct security investigations**		
Level	**6**	**Credits**	**20**

Purpose	This unit standard is for people who conduct, or intend to conduct, security investigations. People credited with this unit standard are able to: - prepare to conduct a security investigation. - gather information and evidence to conduct a security investigation. - analyse and assess information and evidence for a security investigation; and - document and present the results of a security investigation.

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/;
New Zealand Bill of Rights Act 1990;
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;
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
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.
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.
Secure – a state or condition in which risks are minimised.
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.

3 Assessment Range
Evidence of two fully documented security investigations is required.

4 Security investigations cover private, corporate or commercial security investigations.

Outcomes and performance criteria

Outcome 1

Prepare to conduct a security investigation.

Performance criteria

1.1 Establish the terms of reference for the security investigation in accordance with organisational policy and procedures.

Range typical terms of reference may include but is not limited to – objectives of the investigation, acceptable modes of investigation, costs and payment, timing, reporting, possible consequences of the investigation, limitations.

1.2 Identify legal, regulatory, and safety issues together with any special requirements in accordance with organisational policy and procedures.

Range typical special requirements may include but are not limited to – technical support, equipment, liaison and consultation, communications.

1.3 Identify and resolve potential or actual conflicts of interest in accordance with organisational policy and procedures.

1.4 Identify likely sources of information and obtain authorisation where required in accordance with organisational policy and procedures.

Range typical authorities may include but are not limited to – search, interview, consultation, access to and use of information, surveillance.

1.5 Obtain agreement of terms of reference with client and secure authority to proceed.

Outcome 2

Gather information and evidence to conduct a security investigation.

Performance criteria

2.1 Gather information and evidence in accordance with the agreed terms of reference and best practice.

2.2 Conduct investigations with minimal disruption or consequential damage in accordance with the agreed terms of reference and best practice.

2.3 Identify and manage risks to the investigation in accordance with the agreed terms of reference and best practice.

2.4 Record and protect information and evidence in accordance with the terms of reference, rules of evidence, and best practice.

Outcome 3

Analyse and assess information and evidence for a security investigation.

Performance criteria

3.1 Analyse and assess information and evidence to determine their credibility and value in accordance with rules of evidence and best practice.

3.2 Ensure progress reports and reviews are made in accordance with the terms of reference.

3.3 Ensure conclusions and recommendations are consistent with information and evidence, and in accordance with the terms of reference.

Range typical recommendations may include but are not limited to – criminal prosecution; civil, disciplinary or commercial remedies; further investigation; implementation of preventive, deterrent, recovery, or discovery measures.

Outcome 4

Document and present the results of a security investigation.

Performance criteria

4.1 Document and present the results of a security investigation, appropriate to the nature of the investigation 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 but are not limited to– timeliness, content, clarity, conciseness, complexity, level, medium.

4.2 Document and present security investigation 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.

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

Replacement information	This unit standard replaced unit standard 8614.

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.