Whole of Victorian Government Standard
Information Security

Penetration testing

Standard

All externally facing applications and infrastructure, as well as business-assessed sensitive internal systems will be penetration-tested annually.

Keywords:	Penetration testing; pen testing, information security	
Identifier: SEC/STD/03	**Version no:** 1.2	**Status:** Final
Issue date: N/A	**Date of effect:** 13 November 2009	**Next review date:** In progress
Owner: Government Services Division Department of Treasury and Finance Victorian Government	**Issuing authority:** Government Services Division Department of Treasury and Finance Victorian Government	

State Government Victoria

Overview

Information is increasingly being shared within the Victorian Government. While necessary, this practice may expose the Victorian Government to an increased risk of inappropriate information release or access.

The government-wide adoption of common policy, standards and processes for information security will enable the Victorian Government to reduce this risk.

Short description

This standard describes the minimum requirement for Victorian Government departments and agencies to conduct independent penetration testing on their information systems and infrastructure to identify vulnerabilities and weaknesses in security controls.

Context

The standard supports the whole of Victorian Government (WoVG) information security policy: SEC/POL/01: Information Security Management.

Requirements

All externally facing applications and infrastructure, as well as business-assessed sensitive internal systems will be penetration-tested at least annually in accordance with the following requirements.

Priority requirement

Priority must be given to the most critical systems, irrespective of system orientation, i.e. internal or external facing.

A risk assessment must be conducted to determine critical systems. Data classification based on SEC/STD/02[1] is not a sufficient test of criticality as it considers only the confidentiality of the information within the system. Availability and integrity requirements are also important factors to consider.

Frequency requirement

The more critical the system the more frequent and extensive the penetration testing required. At minimum, penetration testing will be undertaken annually, and:

1. after a major security incident, (after the incident has been brought under control, forensic investigations completed and the system stabilised); or
2. following a major change to the system configuration, setup or technology; or
3. following a change in support or outsourcing arrangements.

Testing requirement

Appropriate planning and preparation must be undertaken prior to conducting a penetration test. Considerations may include:

[1] SEC/STD/02: Information Security – Data Classification and Management, April 2009

- impacts, such as degradation of network or system performance, disruption to business operations; and
- legal and contractual implications, such as security clearance of personnel, unintended exposure to sensitive information, and implications for service level agreements.

Penetration testing must be made routine and an integral part of the operations and administration of information systems.

Testing is to be conducted by a reputable, independent party with acknowledged expertise and experience in penetration testing. This party must not have been involved in the design, build or maintenance of the target systems.

The assessment of controls and weaknesses must align with the department's security policy.

Internal and external penetration testing must be performed.

Internal penetration testing will focus on the systems and services accessible and exploitable from inside the network.

External penetration testing will focus on the information, systems and vulnerabilities that are accessible and exploitable from outside the network.

A baseline penetration test must be completed within one year from the date of effect of this standard.

Rationale

Penetration testing:Withdrawn by Enterprise Solutions

- helps safeguard government information;
- improves our understanding of information security threat trends across government;
- detects systemic vulnerabilities;
- provides independent assurance on the adequacy and effectiveness of security controls;
- provides due diligence and compliance to regulators and citizens;
- improves operational information security by identifying vulnerabilities and weaknesses in security controls, and quantifies the impact and likelihood so that proactive corrective measures can be implemented;
- reduces the risk of loss of service for critical internally and externally facing services;
- reduces the risk of significant and adverse public outcomes; and
- protects consumer confidence and government reputation.

Scope

This standard applies to all Victorian Government departments and four inner budget agencies (Environmental Protection Agency, State Revenue Office, VicRoads and Victoria Police).

This standard is the minimum requirement.

This standard does not apply where departments and agencies are subject to legal requirements that contradict or exceed the requirements of this standard; for example, standards issued by the Commissioner for Law Enforcement Data Security (CLEDS) or the requirements of the Information Privacy Act 2000. In such cases, the legal requirements take precedence.

The exploitation of identified external or internal weaknesses and vulnerabilities is beyond the scope of this standard.

Capabilities and limitations awareness

A penetration test is a limited snapshot of the security controls at a given point in time for the systems being tested. Having found no weaknesses or vulnerabilities in a penetration test does not mean that the system is 100 per cent secure.

Guidelines, toolkits and references

This standard supports the WoVG Information Security Management policy (SEC/POL/01). Under this policy, this standard also aligns with:

- SEC/STD/01: Information security management framework; and
- SEC/STD/02: Information security – data classification and management.

Information security is closely related to identity and access management. As such, this standard is also related to and supports the WoVG Identity and Access Management policy (IDAM/POL/01) and standards:

- IDAM/STD/01: IDAM—Staff Authentication—evidence of identity;
- IDAM/STD/02: IDAM—Staff Authentication—authentication mechanism strength;
- IDAM/STD/03: IDAM—Staff Authentication—passwords; and
- IDAM/STD/04: IDAM—Staff Authentication—two factor credentials.

This standard also aligns with:

- the Australian Commonwealth Government's *Protective Security Manual* (PSM)
    - The Commonwealth Government's Attorney General's Department
    - http://www.ag.gov.au/www/agd/agd.nsf/Page/RWPE30AA68A4D5313EACA2571EE000AAF9F
- the Victorian State Government's *Risk Management Framework*
    - The Victorian Department of Treasury and Finance
    - http://www.dtf.vic.gov.au/CA25713E0002EF43/pages/economic-and-financial-policy-victorian-risk-management-framework
- the Standards Australia *Risk Management Standard AS/NZS 4360*

- http://www.standards.org.au/

Templates and guidelines have been developed to assist departments and agencies to implement and report on this standard.

- SEC/GUIDE/03: "Information security penetration testing guideline" assists departments with the implementation of this standard;
- "WoVG Security reporting template" assists departments with reporting intended compliance against this standard; and
- SEC/TEMP/03: "Information security penetration testing compliance reporting template" is the form for reporting testing to GSD.

Further information

For further information regarding this Standard, please contact the Government Services Division, Department of Treasury and Finance on info.cio@dtf.vic.gov.au

Glossary of terms and abbreviations

Term	Meaning
Internal penetration test	Penetration testing the systems and services that are accessible and exploitable from inside an agency level network, and identifying what information and systems can be viewed, and what vulnerabilities exist.
External penetration test	Penetration testing the information, systems and vulnerabilities that are accessible and exploitable from outside the physical bounds of the network. For example, determining what can be identified and accessed from a public network.
Exploitation	Code or technique that is used to take advantage of vulnerability.
Vulnerability	A flaw or weakness that can be exploited to gain an advantage.

Version history

Version	Date	GSD TRIM ref	Details
1.0	13 November 2009	D09/110884	First promulgated
1.1	2 June 2010	D09/110884	Minor changes; specification of reporting dates and templates
1.2	24 March 2011	D09/110884	Aligning reporting to 30 June