Information Security

Business Impact Levels and Other Criteria

Guideline

This guideline specifies business impact levels and other criteria which are intended for use when establishing the consequence and impact of risk in Victorian Government projects, and where a common basis is required across agencies e.g. when agencies cooperate, or share systems or information.

Keywords:	Business impact level, BIL, threat consequence, threat likelihood, risk rating.	
Identifier: SEC GUIDE 02	**Version no.:** 1.0	**Status:** Final
Issue date: 1 September 2012	**Date of effect:** 1 September 2012	**Next review date:** 1 November 2014
Authority: Victorian Government CIO Council	**Issuer:** Victorian Government Chief Technology Advocate	

Overview

As part of the Protective Security Policy Framework (PSPF), the Australian Government has released the *Protective security governance management guidelines - Business impact levels* (BILs) which range from LOW (1) to CATASTROPHIC (6).

These BILs have some potential for re-use within the Victorian Government for the purpose of a Threat Consequence table. When used for the assessment of the impact of disclosure, they also provide guidance for information classification, as the security classifications of PROTECTED, CONFIDENTIAL, SECRET and TOP SECRET directly match to Australian Government BILs 3, 4, 5 and 6 respectively.

The Business Impact levels and other criteria are provided in the appendices of this guideline as follows:

- Appendix 1: Threat consequences, also referred to as Business Impact Levels (BILs)
- Appendix 2: Threat likelihoods
- Appendix 3: Risk Ratings

These criteria:

- are recommended when a common basis is required between any off the eleven departments, Victoria Police, State Revenue Office, VicRoads, Environment Protection Authority, and shared services providers including CenITex. Agencies are free to continue to use their own criteria internally; and
- are guidelines rather than standards, as they address a common 'core' of threat categories only, and there will inevitably be categories of threats that are specific to a project or agency, that are not included in Appendix 1 of this guideline.

Guidelines for use

When assessing common threat consequences (BILs):

- an assessment of the impact should be made for each threat category, and the worst impact across all categories is the minimum impact that should be considered; however

the aggregated threat across **all** impact types should be considered as part of determining the overall impact, and this may encourage a higher impact than the minimum impact.

Rationale

Some projects require the use of common criteria, rather than individual agency criteria:

- Victorian Government (VG) ICT projects require a common VG approach.
- Differences and inconsistencies between agency criteria mean that the criteria to be used in VG projects are unclear.

Even for non-VG projects, a common basis is required when agencies cooperate, or share systems or information.

Derivation

The criteria specified in this guideline are based on *AS/NZS ISO 31000:2009 Risk Management*, and were originally developed for use in the assessment of Victorian Government Critical Information Infrastructure.

- SEC POL 01 Information Security Management Policy;
- SEC STD 01 Information Security Management Framework; and
- SEC STD 02 Critical Information Infrastructure Risk Management

References and toolkits

Information on the development of security risk management plans can be found in the Information Security Risk Management Guidelines available from Standards Australia at: http://www.standards.org.au

Information relating to the Information Security Management Framework is contained in the Australian Government Information Security Management Protocol of the Protective Security Policy Framework.

Victorian Framework for Critical Infrastructure Protection:
http://www.g21.com.au/dmdocuments/HWB-R-0704-167.pdf

Victorian CII Register and CII Health Check templates:
http://digital.vic.gov.au/policies-standards-guidelines/information-security/

Victorian Government Risk Management Framework:
http://www.dtf.vic.gov.au/Publications/Victoria-Economy-publications/Victorian-risk-management-framework-and-insurance-management-policy

Further information

For further information regarding this standard, please contact digital.government@dsdbi.vic.gov.au.

Glossary

Term	Meaning
BIL	Business Impact Level (also called Threat Consequence)
VG	Victorian Government

Version history

Version	Date	TRIM ref	Details
0.1	21 May 2012	n/a	Initial draft
0.2	5 July 2012	D12/157551	Revised draft
1.0	3 August 2012	D12/157551	Final

Appendix 1: Threat Consequences (Business Impact Levels)

Impact Type	Impact Severity				
	Negligible	**Low**	**Medium**	**High**	**Very High**
Safety	First aid treatment only (e.g. band-aid etc.)	Minor medical attention (e.g. stitches by doctor, etc.)	Significant reversible disability (e.g. broken bones, etc.)	One or a few fatalities or one or a few significant irreversible disabilities (e.g. loss of limb etc.)	Many fatalities, and/or many incidents of significant irreversible disabilities
Public Unrest	No / negligible impact on public order, no disruption to community	Minor impact on public order (e.g. peaceful protest with permit), little disruption to community	Measurable impact on public order (e.g. violent local protest, damage to property), some disruption to local community	Prejudice public order (e.g. full blown riot, but localised), significant disruption to local community	Seriously prejudice public order (e.g. widespread rioting, damage to property), extensive disruption to community
Damage to Australian companies	Insignificant impact on financial viability of any Australian based or owned organisation	Undermine the financial viability of, or significantly disadvantage, a minor Australian based or owned organisation	Undermine the financial viability of, or significantly disadvantage, a major Australian based or owned organisation	Undermine the financial viability of, or significantly disadvantage, a few major Australian based or owned organisations	Undermine the financial viability of, or significantly disadvantage, many major Australian based or owned organisations
Confidence in government/ agency	No public concern – attention from one stakeholder with no publicity, routine internal reporting.	Minor damage, visible concern from multiple stakeholders, limited local media interest, specific internal reporting.	Significant short term damage, restricted negative publicity from local media, public embarrassment of agency, internal inquiry	Main stream media reports, intervention of CEO/Secretary, new oversight required, questions in Parliament, external/public inquiry	Broad public concern, national media event, staff/Executive terminations, political resignations, Inquest, Parliamentary Inquiry or Royal Commission
Legal/compliance (including Privacy, legal privilege, commercial confidentiality, contempt, etc.)	Minimal legal/compliance issue, easily resolved. Offence punishable by small fine.	Minor legal issues, non-compliances and/or breaches. Short to medium term action required to resolve. Offence punishable by moderate fine.	Serious failure to comply with legislation/ regulations/ confidentiality. Moderate failure in statutory duty. Immediate action needed to resolve. Offence punishable by major fine. VAGO investigation	Major failure to comply with legislation/ regulations/ confidentiality; breach of Cabinet. Major failure in statutory duty. Shutdown of service for non-compliance. Offence punishable by imprisonment. VAGO investigation	Extreme failure to comply with legislation/ regulation/ confidentiality. Severe failure in statutory duty. Shutdown of >1 service for non-compliance. Major consequences for staff/ agency. VAGO investigation
WoVG Finances	Loss/liability of <0.25% of WoVG annual budget	Loss/liability of 0.25%- < 0.5% of WoVG annual budget	Loss/ liability of 0.5% – < 0.75% of WoVG annual budget	Loss/ liability of 0.75% – < 1% of WoVG annual budget	Loss/ liability of ≥ 1% of WoVG annual budget
Agency Finances	Refer to agency Threat Consequence/BIL table.				

Impact Type	Impact Severity				
	Negligible	**Low**	**Medium**	**High**	**Very High**
Damage to agency assets (beyond financial impact)	Insignificant damage to agency assets	Minor short term damage to agency assets	Significant short term damage to agency assets	Major medium term damage to agency assets	Catastrophic long term damage to agency assets
Service delivery	Refer to agency Threat Consequence/BIL table.				
Crime	Would not assist, or hinder the detection of, any unlawful activity or any crime	Would assist the commission of, or hinder the detection of, unlawful activity (not a crime)	Would facilitate commission of, or impede investigation of, or hinder detection of, low-level crime (not defined in legislation as serious crime). Would hinder the detection of serious crime.	Would facilitate commission of, or impede the investigation of, serious crime (as defined in legislation)	Would directly allow commission of, or prevent investigation of, serious crime (as defined in legislation)
Economy	Insignificant impact on State finances or economic or commercial interests	Minor impact on State finances or economic or commercial interests	Moderate impact on State finances or economic or commercial interests	Work substantially against State finances or economic or commercial interests	Substantial damage to State finances or economic or commercial interests
Relationships with other governments	Insignificant or no damage to relations between the Victorian Government and other (federal, state or territory, or international) governments	Would cause minor damage to relations between the Victorian Government and other (federal, state or territory, or international) governments	Would cause moderate damage to relations between the Victorian Government and other (federal, state or territory, or international) governments	Would cause major damage to relations between the Victorian Government and other (federal, state or territory, or international) governments	Would result in termination of some aspects of relations between the Victorian Government and other (federal, state or territory, or international) governments
Agency operations or programs	Insignificant impact, resolved by routine operations	Some degradation, minor impact on efficiency or effectiveness, managed internally	Significant degradation, impedes effective operation, significant review/ changes required	Severe degradation, seriously impedes operation, service/ project/ program may not survive	Halt of operations, agency/ business unit may not survive
Harm to the environment	Single incident resulting in no material environmental harm	Minor, transient environmental harm	Environmental harm that takes up to 2 years to reverse	Environmental harm that takes 2 – 5 years to reverse	Irreversible environmental harm and/or environmental harm that takes >5 years to reverse
Disclosure Impact		UNCLASSIFIED INFORMATION		CLASSIFIED INFORMATION	
Security Classification	**PUBLIC DOMAIN** or unlabelled	**UNCLASSIFIED** or unlabelled	DLM Only: **For Official Use Only**, **Sensitive**, or **Sensitive: X**	**PROTECTED** (may also have DLM of **Sensitive: Cabinet**)	**PROTECTED**

Appendix 2: Threat Likelihoods (sample for workshops)

Likelihood	Description	Example frequency
Almost certain	Risk occurring now, is expected to occur in most circumstances.	Once (or more) a week
Likely	Will probably occur in most circumstances.	Once a month
Possible	May occur at some time.	Once a year
Unlikely	Not generally expected, but may occur.	Once in 3 years
Rare	May only occur in exceptional circumstances	Once in more than 3 years

Appendix 3: Risk Ratings Table (sample for workshops)

		Threat Consequence				
		Negligible	**Low**	**Medium**	**High**	**Very High**
Threat Likelihood	**Almost certain**	Medium	High	High	Extreme	Extreme
	Likely	Medium	Medium	High	High	Extreme
	Possible	Low	Medium	Medium	High	High
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Low	Medium	High