



**Office of the Victorian  
Information Commissioner**

## **Practitioner Guide:**

# **Assessing the Security Value of Public Sector Information**

- **Conducting an information security value assessment (using Business Impact Levels)**
- **Determining the overall security value of public sector information**

*(Formerly Chapter 2 of the Information Security Management Collection)*

**Version 2.0 November 2019**

Published by the Office of the Victorian Information Commissioner

PO Box 24274

Melbourne Victoria 3001

First published June 2016

Amended November 2019

Also published on: <https://ovic.vic.gov.au>

ISBN 978-0-6486723-4-0



You are free to re-use this work under a Creative Commons Attribution 4.0 licence, provided you credit the State of Victoria (Office of the Victorian Information Commissioner) as author, indicate if changes were made and comply with the other licence terms. The licence does not apply to any branding, including Government logos.

**Practitioner Guide Details**

<b>Assessing the Security Value of Public Sector Information</b> <i>(formerly Chapter 2 of the VPDSF Information Security Management Collection)</i>	
Protective Marking	N/A
Approved for unlimited public release?	<i>Yes – Authorised for release</i>
Release Date	November 2019
Review Date	November 2020
Document Version	2.0
Authority	Office of the Victorian Information Commissioner (OVIC)
Author	Information Security Unit – OVIC

For further information, please contact the Information Security Unit on [security@ovic.vic.gov.au](mailto:security@ovic.vic.gov.au)

## Table of Contents

1. Background .....	5
2. Purpose.....	5
3. Audience.....	5
4. Use of specific terms in this document.....	5
5. Scope .....	5
6. What information needs to undergo a security value assessment?.....	5
7. Who performs an information security value assessment?.....	6
7.1. The assessment process .....	6
8. Assessment Considerations.....	8
8.1. Legislative requirements governing the information.....	9
8.2. Inappropriate use of protective markings.....	9
8.3. Prevent over-classification .....	9
8.4. Consider the combined security value of the information .....	9
9. Victorian versus Commonwealth scheme .....	10
9.1. VPDSF (Victorian) vs. PSPF (Commonwealth) BILs.....	10
10. Business Impact Levels (BILs) .....	12
10.1. What are Business Impact Levels (BILs)?.....	12
10.2. Why use BILs?.....	12
10.3. What is the VPDSF BIL table?.....	12
11. How to read the VPDSF BIL table .....	13
11.1. Impact levels .....	13
11.2. Impact categories.....	13
11.3. Impacts.....	13
12. Contextualising the VPDSF BIL table for an organisation .....	13
13. Working examples – Conducting an information security valuation assessment .....	16
14. Information lifecycle and security value assessments .....	22
Appendix A – Performing an information security value assessment .....	23
Appendix B – VPDSF Business Impact Level (BIL) Table .....	24

## 1. Background

The Office of the Victorian Information Commissioner (OVIC) issues security guides to support the Victorian Protective Data Security Standards (VPDSS). All guidance documents and references are inter-linked and should not be read in isolation.

This document forms part of a suite of supporting security guides of the VPDSS.

## 2. Purpose

Everyone who works with public sector information has an obligation to respect the information that they create, access and use, and are personally accountable for safeguarding this material. A fundamental starting point in developing a positive security culture across the Victorian public sector, is understanding the security value of the information we work with. To do this, organisations need to train their personnel in performing consistent information security value assessments, and apply the appropriate security measures to maintain the confidentiality, integrity and availability of public sector information.

This document aims to assist organisations by:

- providing guidance about assessing public sector information using a consistent impact assessment tool (taking the form of Business Impact Levels – BILs<sup>1</sup>);
- contextualising the VPDSF BILs in line with the organisation’s specific operating requirement;
- determining the overall security value of public sector information;
- identifying the appropriate protective marking for the information; and
- understanding if additional security measures are required to protect public sector information (beyond those security measures already informed by the protective marking).

## 3. Audience

This document is intended for Victorian public sector organisations (including employees, contractors and external parties) that are subject to the protective data security provisions under Part Four of Victoria’s Privacy and Data Protection Act (2014).

This guide is designed to support practitioners and information security leads.

## 4. Use of specific terms in this document

Please refer to the *VPDSF Glossary of Protective Data Security Terms* for an outline of terms and associated definitions. For a current copy of this document, please refer to the VPDSF Resources section of the OVIC website.

## 5. Scope

This document directly supports the Victorian Protective Data Security Standards (VPDSS), and informs step two the VPDSS Five Step Action Plan<sup>2</sup>. Assessing the ‘security value’ of public sector information.

## 6. What information needs to undergo a security value assessment?

---

<sup>1</sup> Business Impact Levels (BILs) describe scaled impacts which would be expected to cause harm or damage to government operations, organisations or individuals, if there were a compromise of the confidentiality, integrity and/or availability of public sector information.

<sup>2</sup> For more information, refer to the *Five Step Action Plan* which can be found under the VPDSF Resources section of the OVIC website.

An information assessment must only be performed on public sector information. To help distinguish between ‘public sector information’ and ‘unofficial’ information, the following definitions are offered:

**‘Public sector information’**

Any information (including personal information) obtained, generated, received or held by or for an applicable Victorian public sector organisation for an official purpose or supporting official activities. This includes both hard and soft copy information, regardless of media or format.

Each item or record that makes up an information asset needs to be independently assessed, valued and have a protective marking applied if required.

**‘Unofficial’ information**

Information that has no relation to official activities, such as a personal correspondence. Unofficial information does not need to undergo a security value assessment.

‘Unofficial’ information has no bearing on official functions and, as such, is automatically assigned a BIL of zero. ‘Unofficial’ information must not have a protective marking applied to it<sup>3</sup>.

**7. Who performs an information security value assessment?**

The person or organisation, responsible for preparing, creating or actioning public sector information is best placed to conduct an assessment of the material, in order to determine it’s ‘security value’. This person or organisation is commonly referred to as ‘the originator’.

This person, or organisation, is also responsible for deciding whether, and at what level, to value information, by completing the information assessment process. It is the responsibility of the originator to ensure any recipients of the information they create, understand how to protect the information.

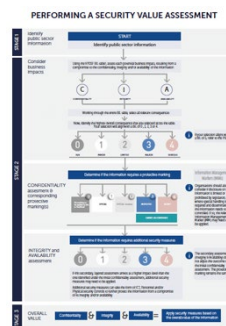
**7.1. The assessment process**

In order to determine the ‘security value’ of information, originators must conduct an assessment which is set out across three stages -

**Stage 1**    Review the content

**Stage 2**    Consider potential impacts if the information was compromised


**Stage 3**    Understand the overall security value of the information, in order to apply the appropriate security measures



Refer to *Appendix A* of this guide for a visual representation of this assessment process.

<sup>3</sup> Whilst ‘Unofficial’ is not recognised as a formal protective marking, it is used for email marking purposes. For email marking guidance refer to your organisation’s internal policies and procedures and IT Team.

## PERFORMING AN INFORMATION SECURITY VALUATION ASSESSMENT


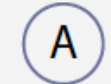
<p><b>STAGE 1</b></p> <p><b>Review the content</b></p>	<p>Start off by reviewing the content<sup>4</sup>. By understanding the content, an originator<sup>5</sup> is able to assess potential impact(s) if there were a compromise to this material.</p> <p>N.B. An information security value assessment is only performed on public sector information. If the material is deemed ‘unofficial’, a security value assessment does not need to be undertaken, or a protective marking applied.</p>
<p><b>STAGE 2</b></p> <p><b>Consider potential business impacts</b></p>	<p>Assess the potential business impacts to government operations, organisations or individuals, if there was a compromise to the:</p> <ul style="list-style-type: none"> <li>• <i>Confidentiality (C)</i></li> <li>• <i>Integrity (I)</i></li> <li>• <i>Availability (A)</i></li> </ul> <p>of the information.</p>
<p><b>STAGE 2.1</b></p> <div style="text-align: center; margin: 10px 0;">  </div> <p><b>Confidentiality assessment</b></p>	<p>Confidentiality refers to the limiting of access of public sector information to authorised persons, for approved purposes.</p> <p>In this stage of the assessment process, the originator considers potential impact(s) of unauthorised disclosure of the information. To do this the originator assesses the degree to which, and the extent or duration of, any impacts any impacts if there were a compromise of the <i>confidentiality</i> of the information.</p> <p>The outcome of the confidentiality assessment directly informs the protective marking(s)<sup>6</sup> for the information.</p>

---

<sup>4</sup> ‘Content’ refers to the information captured within a document, email, spreadsheet, audio recording, imagery or information that is verbally disclosed.

<sup>5</sup> The originator of the information is responsible for preparing/creating public sector information or for actioning information generated outside the public sector (i.e. material generated by private industry).

<sup>6</sup> For more information on protective markings, refer to VPDSF Practitioner Guide: Protective Markings

<p><b>STAGE 2.2</b></p>  <p><b>Integrity assessment</b></p>	<p>Integrity refers to the assurance that public sector information has been created, amended or deleted only by the intended authorised means and is correct and valid.</p> <p>In this stage of the assessment process, the originator considers potential impact(s) of unauthorised modification of the information and the significance of this to government operations, organisations or individuals.</p> <p>To do this the originator assesses the degree to which, and the extent or duration of, any impacts if there were a compromise of the <i>integrity</i> of the information.</p> <p>The outcome of the integrity assessment establishes whether additional security measures are required, beyond those established by the protective marking.</p>
<p><b>STAGE 2.3</b></p>  <p><b>Availability assessment</b></p>	<p>Availability refers to ensuring authorised persons access to public sector information for authorised purposes, at the time they need to do so.</p> <p>In this stage of the assessment process, the originator considers potential impact(s) of unauthorised unavailability of the information and the significance of this to government operations, organisations or individuals.</p> <p>To do this the originator assesses the degree to which, and the extent or duration of, any impacts if there were a compromise of the <i>availability</i> of the information.</p> <p>The outcome of the availability assessment establishes whether additional security measures are required, beyond those established by the protective marking.</p>
<p><b>STAGE 3</b></p> <p><b>Understand the overall security value and apply security measures</b></p>	<p>The information assessment process delivers three equally important outcomes:</p> <ol style="list-style-type: none"> <li>1. The protective marking(s) needed for the information <i>(based on the confidentiality assessment)</i></li> <li>2. An understanding of whether any additional security measures are needed to further protect the information beyond the protective marking <i>(based on the integrity and availability assessments)</i></li> <li>3. The overall ‘security value’ of the information <i>(based on the highest overall impact drawn from each of the the confidentiality, integrity and availability assessments)</i></li> </ol>

## 8. Assessment Considerations



When assessing public sector information, the originator should keep in mind the following.

### **8.1. Legislative requirements governing the information**

Some forms of public sector information are governed by legislation that restricts or prohibits disclosure of its content, imposes certain use and handling requirements or restricts distribution of the material<sup>7</sup>.

Be aware of any legislative requirements relating to the information when performing a security value assessment as it may help inform which protective marking is needed / appropriate for particular content types.

### **8.2. Inappropriate use of protective markings**

Public sector information should only be protectively marked where there is a clear and justifiable need to do so (i.e. an information security value assessment has determined a protective marking is required).

In no case should public sector information be protectively marked to:

- hide violations of law, inefficiency or administrative error;
- prevent embarrassment to an individual, organisation;
- restrain competition; or
- prevent or delay the release of information that does not need protection.

The presence or absence of a protective marking does not affect a document's status under Freedom of Information (FOI) Act.

### **8.3. Prevent over-classification**

It is important that only information requiring some form of protection is labelled with a protective marking. In particular, security classifications (a form of protective marking) should only be used where compromise of the confidentiality of the information warrants increased protection.

Inappropriate over classification can result in:

- access to public sector information being unnecessarily limited or delayed;
- overly onerous administration and procedural overheads, imposing additional costs on the organisation; and
- protective markings being devalued or ignored by personnel and receiving parties.

### **8.4. Consider the combined security value of the information**

Where multiple pieces of public sector information are stored together, the overall security value of this combined material need to be considered. Risks associated with these combined pieces of information may be higher than any single instance or individual record. As such additional security measures may be needed to protect these combined (aggregated) information assets.

This is particularly important when selecting particular types of equipment, systems, facilities or services

---

<sup>7</sup> For more information on some of the more common legislative requirements governing information and available protective markings, refer to *VPDSF Practitioner Guide: Protective Markings*. For a current copy of this document, please refer to the VPDSF Resources section of the OVIC website.

needed to protect this information, as extra security controls may be required.

### 9. Victorian versus Commonwealth scheme

Different regulatory arrangements exist governing the oversight and management of public sector information across jurisdictions (i.e. State / Territory versus Commonwealth).

With in Victorian Government, Business Impact Levels (BILs) are used to assess public sector information. This approach is consistent with the Commonwealth Protective Security Policy Framework (PSPF) who also employs this method. By adopting a consistent assessment tool, Victorian public sector organisations are positioned to effectively share information across jurisdictions without having to undergo complex mapping exercises.

Prior to conducting a security value assessment, organisations need to first consider which scheme to apply. Ask yourself, ‘does this information have the potential to affect national interest?’ If yes, refer to the PSPF.

National interest refers to matters that have or could have impact on Australia, including:

- national security
- international relations
- law and governance, including:
  - State / territory relations
  - law enforcement operations where compromise could hamper or prevent national crime prevention strategies or investigations or endanger personal safety
- economic wellbeing
- heritage or
- culture

A visual representation of this consideration is provided in *Figure 2*, along with a brief description of the two complementary schemes (Victorian and Commonwealth).

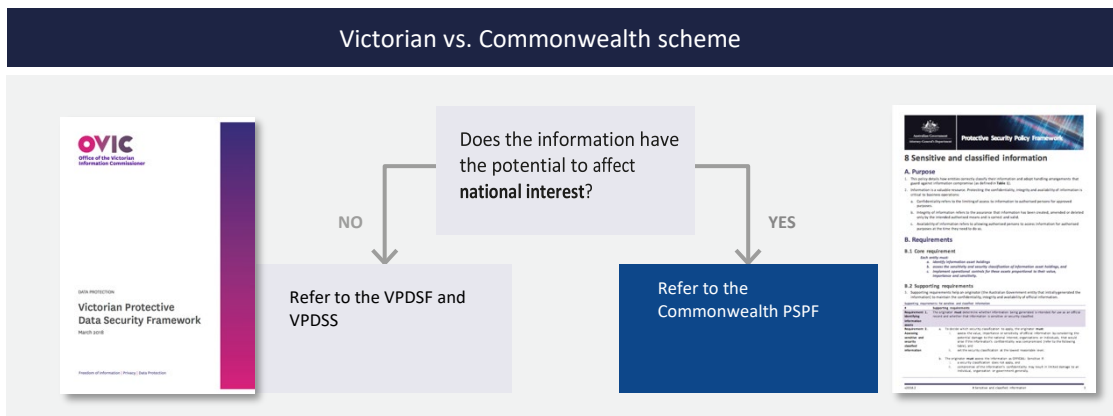


Figure 2 – Does the information have the potential to affect National Interest?

#### 9.1. VPDSF (Victorian) vs. PSPF (Commonwealth) BILs

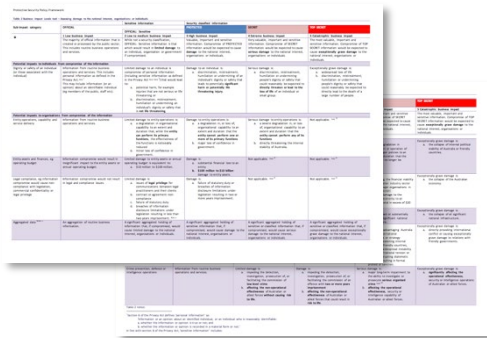


### VPDSF (State) BILs

The VPDSF BIL table has been developed to provide a basis for Victorian public sector organisations to assess the security value of public sector information.

The VPDSF BIL table referenced in *Appendix B* of this guide, provides organisations with scaled impact levels and categories to use to assess a compromise of the confidentiality, integrity or availability of public sector information.

As already noted, if the information has the potential to affect the ‘national interest’, immediately refer to the PSPF.



### PSPF (Commonwealth) BILs

A limited number of Victorian organisations will create, use or receive information that could impact on Australia’s national interest.

Where information is assessed as having the potential to impact ‘national interest’, organisations are to adhere to the requirements set out in the PSPF (*Protective security governance guidelines – Business Impact Levels*).

The PSPF provides its own BIL table with its own set of definitions and impacts.

For more information of the PSPF, refer the PSPF website at [www.protectivesecurity.gov.au](http://www.protectivesecurity.gov.au)

## 10. Business Impact Levels (BILs)

In order to undertake a consistent information security value assessment, organisations should use a common security valuation criteria called Business Impact Levels (BILs). By undertaking this assessment, organisations can determine the security value of public sector information.

### 10.1. What are Business Impact Levels (BILs)?

BILs are quantitative measures of scaled impacts, that describe the potential impact arising from a compromise of the -

- Confidentiality
- Integrity and / or
- Availability

of public sector information.

The VPDSF BIL table is set out in *Appendix B* of this document.



### 10.2. Why use BILs?

BILs help organisations assess and communicate the impact(s) of particular information impacts with internal stakeholders, linked organisations, business partners, external parties and providers.

By assessing public sector information in a standardised manner, Victorian public sector organisations are able to consider, and collaboratively manage, information security risks. This provides a solid foundation for secure information sharing practices and allows organisations to share information using commonly understood terms. This fosters informed discussions over what the security measures needed to securely share public sector information.

### 10.3. What is the VPDSF BIL table?

The VPDSF BIL table (refer to *Appendix B* of this document) provides:

- **scaled impact levels** that describe harm or damage to government operations, organisations or individuals
  - under the VPDSF BIL table, these impacts levels commence at zero and scale through to a maximum of four. They are presented across the top of the BIL table.
  - a fifth level is presented on the VPDSF BIL table, however this level is reserved for matters of ‘national interest’. Organisations should refer to the Commonwealth PSPF if they feel the information they are assessing fits this criteria
- **impact categories**
  - grouped impact types, listed down the left-hand side of the BIL table
- **impact statements**
  - presented across each category and scaled across each of the levels

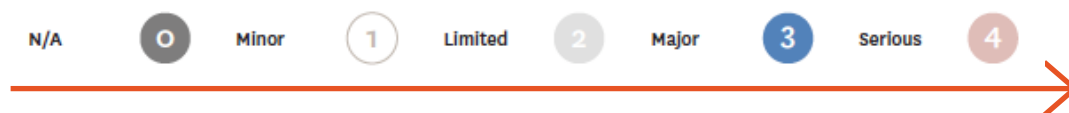
It is important to note that the BIL table is not a risk table / matrix. The BIL table does not take into account the likelihood of something occurring, just the impact if something were to occur.

## 11. How to read the VPDSF BIL table

### 11.1. Impact levels

An impact level summarises the:

- severity of potential impacts; and
- degree to which a compromise of public sector information is likely to cause harm or render damage.



As potential impact(s) increase in severity, the levels rise.

*N.B. The BIL of 5 is not presented in the above visual, as this relates to matters of national interest. Refer to the Commonwealth PSPF if information fits these criteria.*

### 11.2. Impact categories

In the VPDSF BIL table, impacts with 'like attributes' are grouped into categories. Examples of impact categories include:

- Economy and Finance
- Legal and Regulatory
- Personal
- Public Services
- Public Order, Public Safety and Law Enforcement

### 11.3. Impacts

The VPDSF BIL table presents standardised impact statements describing adverse effects or results, rendering harm or damage, if the confidentiality, integrity or availability of public sector information were compromised.

## 12. Contextualising the VPDSF BIL table for an organisation

Victorian public sector organisations are expected to use the VPDSF BIL table (*Appendix B* of this document) to assess any impacts resulting from a compromise to the confidentiality, integrity and availability of public sector information.

The VPDSF BIL table should not be adjusted, as pre-defined impact statements and levels provide a standardised model for Victorian public sector organisations to utilise. The fixed nature of these statements is critical to ensuring organisations use consistent valuation criteria when assessing public sector information, and in turn, communicating its sensitivities and significance in a standardised manner.

Rather, Victorian organisations should consider the standardised impact statements in the context of their specific operating requirements. These considerations may be influenced by their functions, size, resources or information assets.

Where sample impacts are presented in the VPDSF BIL table (e.g. organisation's operating budget), organisations should reflect on their own operating context and interchange that standardised impact

descriptions with a reference that suitably describes the actual impact and implication to their business. Not all impact statements presented in the VPDSF will require this contextualization, but some will.

External parties with access (direct or indirect) to public sector information should also refer to the BIL table of the engaging Victorian public sector organisation. For queries on how to use the BIL table, external parties are encouraged to seek guidance from the engaging VPS organisation.

**Example 1 – Contextualising the sub impact category of ‘Organisation’s operating budget’**

	Impact Levels						
	N/A	0	1	2	3	4	5
	No business impact	Minor Compromise of the information would be expected to cause <b>minor</b> harm/damage to government operations, organisations or individuals, resulting in one or more of the following:	Limited Compromise of the information would be expected to cause <b>limited</b> harm/damage to government operations, organisations or individuals resulting in one or more of the following:	Major Compromise of the information would be expected to cause <b>major</b> harm/damage to government operations, organisations or individuals, resulting in one or more of the following:	Serious Compromise of the information would be expected to cause <b>serious</b> harm/damage to government operations, organisations or individuals in one or more of the following:	Exceptional Compromise of the information would be expected to cause <b>exceptionally</b> grave damage to the national interest	
Economy And Finance							
Organisation's operating budget (impact on public finances)	N/A	+ Loss of < 1% of a government organisation's annual operating budget	+ Loss of > 1% – 10% of a government organisation's annual operating budget	+ Loss of > 10% – 20% of a government organisation's annual operating budget + Short-term material impact on State finances or economy	+ Loss of ≥ 20% of a government organisation's annual operating budget + Long-term damage to State finances or economy	Refer to Commonwealth Protective Security Policy Framework (PSPF)	

The VPDSF BIL table presents standardised financial impact statements, scaling from ‘Minor’ impact through to ‘Serious’. Each descriptor is accompanied by a percentage (%) figure, quantifying scaled business impacts for a loss to the organisation’s annual operating budget.

A certain percentage loss will have different implications for different organisations – i.e. losing >1% – 10% of a smaller government organisation’s annual operating budget would have a very different effect to that of a larger organisation which may be able to absorb the financial impact better.

In order for an organisation to consider the standardised impacts in the context of their specific operating requirements, they need to first consider their own overall operating budget.

For example, the operating budget of Agency X is \$4,000,000. Using the VPDSF BIL table, Agency X would interchange the VPDSF BIL percentages with their equivalent financial amount(s) for that impact level, drawn from the organisation’s annual operating budget.

The below statements have been contextualised, based on Agency X’s \$4,000,000 annual operating budget:

N/A	0	Minor 1	Limited 2	Major 3	Serious 4
Resulting in no loss, as there is no business impact, because the information in this category describes content that is ‘Unofficial’	Resulting in an Minor loss of less than \$40,000 of the organisation’s annual operating budget	Resulting in a limited loss of \$40,000 – \$400,000 of the organisation’s annual operating budget	Resulting in a major loss of \$400,000 – \$800,000 of the organisation’s annual operating budget	Resulting in a serious loss of greater than \$800,000 of the organisation’s annual operating budget	

**Example 2 – Contextualising the sub impact category of ‘Legal / Compliance’**

	Impact Levels									
	N/A	0	Minor 1	Limited 2	Major 3	Serious 4	Exceptional 5			
	No business impact	Compromise of the information would be expected to cause <b>minor</b> harm/damage to government operations, organisations or individuals, resulting in one or more of the following:	Compromise of the information would be expected to cause <b>limited</b> harm/damage to government operations, organisations or individuals resulting in one or more of the following:	Compromise of the information would be expected to cause <b>major</b> harm/damage to government operations, organisations or individuals, resulting in one or more of the following:	Compromise of the information would be expected to cause <b>serious</b> harm/damage to government operations, organisations or individuals in one or more of the following:	Compromise of the information would be expected to cause <b>exceptionally</b> grave damage to the national interest				
<b>Legal and Regulatory</b>										
<b>Legal/compliance</b>  (including applicable legislation and agreements or contracts)  E.g. Non-compliance with legislation, commercial confidentiality and legal privilege	N/A	No compliance issue or breach	+ Non-compliance with contracts or agreements + Failure of statutory duty + Issues of legal privilege for communications between legal practitioners and their clients + Violation of confidentiality or secrecy provisions in legislation resulting in less than two years imprisonment + Misconduct investigation managed internally	+ Non-compliance with contracts or agreements + Failure of statutory duty + Issues of legal privilege for communications between legal practitioners and their clients + Violation of confidentiality or secrecy provisions in legislation, resulting in less than two years imprisonment + Misconduct investigation managed either internally or externally	+ Non-compliance with contracts or agreements + Failure of statutory duty + Issues of legal privilege for communications between legal practitioners and their clients + Violation of confidentiality or secrecy provisions in legislation, resulting in more than two years imprisonment	+ Non-compliance with contracts or agreements + Failure of statutory duty + Issues of legal privilege for communications between legal practitioners and their clients + Violation of confidentiality or secrecy provisions in legislation, resulting in more than two years imprisonment	<b>Refer to Commonwealth Protective Security Policy Framework (PSPF)</b>			

The VPDSF BIL table presents standardised legal and regulatory impact statements, scaling from ‘Minor’ through to ‘Serious’.

Under the sub impact category of ‘Legal/Compliance’, some standardised legal or compliance impact statements have been presented. These impacts could include non-compliance with legislation, commercial confidentiality and legal professional privilege.

The complex legal and regulatory landscape in which Victorian organisations operate, means different agencies or bodies are required to observe a range of compliance requirements. These requirements will change from organisation to organisation (e.g. ‘small and simple’ to ‘large and complex’) and are significantly influenced by the requirements of the legislation they administer or operate under.

In order for an organisation to understand how to apply the standardised impacts from the VPDSF BIL table, they first need to consider the legal and regulatory environment in which they operate.

For example, compliance obligations for a single entity may include, but are not limited to:

- Public Administration Act (2004)
- Public Records Act (1973)
- Financial Management Act (1994)
- Privacy and Data Protection Act (2014)
- Freedom of Information Act (1982)
- Local operating agreements, arrangements or contracts

Understanding these obligations, will help contextualise what a ‘minor, limited, major, and serious’ legal / compliance impact would be, in relation to their own operating environment.

### 13. Working examples – Conducting an information security valuation assessment

The following section provides two working examples under which an organisation conducts an information security valuation assessment using the VPDSF BIL table. These are only sample representations of how to conduct an information assessment.

#### EXAMPLE 1 – OFFICE OF THE VICTORIAN INFORMATION COMMISSIONER (OVIC)



The Office of the Victorian Information Commissioner (OVIC) conducts a security review on a potential breach of public sector information from a government agency.

The team create a file note summarising the breach and need to determine:

- if the information requires a protective marking; and
- whether any additional security measures are required to further protect this information, beyond those established by the protective marking.



#### Confidentiality assessment


The team conducts an initial assessment to consider what the potential impacts would be, if the **confidentiality** of the information was compromised. This assessment will help determine the relevant business impact level (BIL) for this stage.

After assessing each of the impact statements in the BIL table, multiple outcomes are identified.

These outcomes highlighted that the need for the information to remain confidential, as unauthorised access could be expected to cause **major (BIL of 3)** harm/damage to government operations, organisations or individuals.

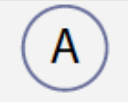









Potential impacts included **major (BIL of 3)**:



	<ul style="list-style-type: none"> <li>• legal and compliance implications (non-compliance with confidentiality and secrecy provisions in legislation);</li> <li>• reputational damage;</li> <li>• broad public concern;</li> <li>• mainstream media reports and negative publicity; and/or</li> <li>• damage to crime fighting including impeding the investigation of an indictable offence.</li> </ul>
<p><b>Confidentiality result</b></p>	<p>A compromise to the confidentiality of this public sector information was assessed at a <b>major</b> business impact level (<b>BIL of 3</b>).</p> <p>Confidentiality impacts at this level, correspond with a security classification of <b>'PROTECTED'</b>. Depending on the content, the information could also be labelled with additional Information Management Markers<sup>8</sup>.</p>
<div style="text-align: center;">  <p><b>Integrity assessment</b></p> </div>	<p>The team then conducts a secondary assessment of the same information to consider what impacts could occur if the <b>integrity</b> of the material was compromised.</p> <p>After assessing each of the impact statements in the BIL table, <b>limited (BIL of 2)</b> outcomes were identified. These outcomes were based on the need for the OVIC team to readily access accurate information.</p> <p>Potential impacts included <b>limited (BIL of 2)</b>:</p> <ul style="list-style-type: none"> <li>• damage to an organisation's assets; and/or</li> <li>• degradation or cessation of non-critical (non-essential or important) business operations, systems or services, to an extent that while the organisation can perform its primary functions, the efficiency and effectiveness of the functions is noticeably reduced or impeded.</li> </ul>
<p><b>Integrity result</b></p>	<p>A compromise to the integrity of the public sector information was assessed as a <b>limited</b> business impact level (<b>BIL of 2</b>).</p>

---

<sup>8</sup> For more information on information management markers, refer to *VPDSF Practitioner Guide: Protective Markings*. For a current copy of this document, please refer to the VPDSF Resources section of the OVIC website.

<div style="text-align: center;">  <p><b>Availability assessment</b></p> </div>	<p>The team then conducts a final assessment of the same information to consider what impacts could occur if the <b>availability</b> of the material was compromised.</p> <p>After assessing each of the impact statements in the BIL table, <b>limited (BIL of 2)</b> outcomes were identified. These outcomes were based on the need for the OVIC team to readily access up to date information.</p> <p>Potential impacts included <b>limited (BIL of 2)</b>:</p> <ul style="list-style-type: none"> <li>• damage to an organisation’s assets; and/or</li> <li>• degradation or cessation of non-critical (non-essential or important) business operations, systems or services, to an extent that while the organisation can perform its primary functions, the efficiency and effectiveness of the functions is noticeably reduced or impeded.</li> </ul>						
<div style="text-align: center;"> <p><b>Availability result</b></p> </div>	<p>A compromise to the <b>availability</b> of the public sector information was assessed as a <b>limited</b> business impact level (<b>BIL of 2</b>).</p>						
<div style="text-align: center;"> <p><b>Overall assessment result</b></p> </div>	<p>In this working example, the <b>overall security value</b> of the information was a <b>BIL of 3</b>. This was based on the selection of the <b>highest BIL</b> from each of the three assessments (i.e. confidentiality, integrity and availability).</p> <table border="1" data-bbox="456 1111 1331 1424"> <tr> <td style="text-align: center;">   <small>CONFIDENTIALITY</small> </td> <td>(<b>BIL</b>) of 3 Corresponding protective marking of <b>PROTECTED</b> to be applied to the content</td> </tr> <tr> <td style="text-align: center;">   <small>INTEGRITY</small> </td> <td>(<b>BIL</b>) of 2 N.B. The outcomes of this assessment do not alter the protective marking</td> </tr> <tr> <td style="text-align: center;">   <small>AVAILABILITY</small> </td> <td>(<b>BIL</b>) of 2 N.B. The outcomes of this assessment do not alter the protective marking</td> </tr> </table> <p>As the ‘<i>integrity</i>’ and ‘<i>availability</i>’ BILs (<b>BIL of 2</b>) are lower than ‘<i>confidentiality</i>’ BIL (<b>BIL of 3</b>), additional security measures beyond those imposed by the <b>PROTECTED</b> security classification, do not need to be considered in this instance.</p> <p>In summary, OVIC should implement security controls that accompany a security classification of <b>PROTECTED</b>. These security measures include personnel, ICT and physical security controls.</p> <p>The team still need to be mindful of any legislative obligations governing the management of the information, and the application of additional information management markers (IMMs) to signify this, and help manage the information.</p>	 <small>CONFIDENTIALITY</small>	( <b>BIL</b> ) of 3 Corresponding protective marking of <b>PROTECTED</b> to be applied to the content	 <small>INTEGRITY</small>	( <b>BIL</b> ) of 2 N.B. The outcomes of this assessment do not alter the protective marking	 <small>AVAILABILITY</small>	( <b>BIL</b> ) of 2 N.B. The outcomes of this assessment do not alter the protective marking
 <small>CONFIDENTIALITY</small>	( <b>BIL</b> ) of 3 Corresponding protective marking of <b>PROTECTED</b> to be applied to the content						
 <small>INTEGRITY</small>	( <b>BIL</b> ) of 2 N.B. The outcomes of this assessment do not alter the protective marking						
 <small>AVAILABILITY</small>	( <b>BIL</b> ) of 2 N.B. The outcomes of this assessment do not alter the protective marking						

EXAMPLE 2 – COUNTRY FIRE AUTHORITY (CFA)



The Country Fire Authority (CFA) regularly publishes important information on their website notifying members of the community about fire warnings, incidents and planned burns.

The CFA team are looking to publish updated material about a fire warning on their website, however prior to doing this they need to determine:

1. If the information requires a protective marking; and
2. Whether any additional security measures are required to further protect this information, beyond those established by the protective marking.



**Confidentiality assessment**

The team conduct an initial assessment to consider the potential impacts, if the **confidentiality** of the information was compromised. This assessment will help determine the relevant impact level for this stage.

After assessing each of the impact statements in the BIL table, **minor (BIL of 1)** outcomes were determined.

These potential impacts identified an unauthorised release of the information could be expected to cause only **minor** harm/ damage to government operations, organisations and individuals resulting in a **BIL of 1**.

Additional considerations included:

- the authorising environment of the agency, which had approved this content for public release (authorisation);
- that this information was initially created/ designed for members of the public to consume (purpose); and
- the agency (CFA) need to ensure all persons (public and VPS) have unrestricted access to the information presented on their corporate website (intent).

**Confidentiality result**

In this example, a compromise to the **confidentiality** of the information was assessed as a **BIL of 1**.

Information assessed at this level often bears a protective marking of **OFFICIAL**<sup>9</sup>, but may be suitable for release to the public, once authorised by appropriate representatives within the CFA.




<sup>9</sup> Refer to VPDSF Practitioner Guide: Protective Markings for further information

<div data-bbox="225 237 363 331" data-label="Image"> </div> <p data-bbox="220 387 368 450"><b>Integrity assessment</b></p>	<p data-bbox="472 241 1390 349">The team then conducts a secondary assessment of the same information to consider what impacts could occur if the <b>integrity</b> of the material was compromised.</p> <p data-bbox="472 387 1390 533">After assessing each of the impact statements in the BIL table, major (BIL of 3) outcomes were identified. These outcomes took into account the need for the public and partnering agencies to <b>access up-to-date and accurate</b> information from the CFA website.</p> <p data-bbox="472 571 995 600">Potential impacts included <b>major (BIL of 3)</b>:</p> <ul data-bbox="472 638 1374 824" style="list-style-type: none"> <li>• compromise of individuals personal safety and wellbeing if incorrect or outdated information were provided on the CFA website during an emergency period; and/or</li> <li>• disruption to the community if people received altered or falsified information from the CFA website.</li> </ul>
<p data-bbox="201 891 387 920"><b>Integrity result</b></p>	<p data-bbox="472 891 1390 965">A compromise to the <b>integrity</b> of the public sector information was assessed as a <b>major</b> business impact level <b>(BIL) of 3</b>.</p>
<div data-bbox="225 1059 363 1153" data-label="Image"> </div> <p data-bbox="220 1216 368 1279"><b>Availability assessment</b></p>	<p data-bbox="472 1064 1342 1171">The team then conducts a final assessment of the same information to consider what impacts could occur if the <b>availability</b> of the material was compromised.</p> <p data-bbox="472 1209 1382 1355">After assessing each of the impact statements in the BIL table, <b>major (BIL of 3)</b> outcomes were identified. These outcomes were based on the need for the public and partnering agencies to <b>readily access up to date</b> information from the CFA website.</p> <p data-bbox="472 1393 995 1422">Potential impacts included <b>major (BIL of 3)</b>:</p> <ul data-bbox="472 1460 1390 1720" style="list-style-type: none"> <li>• compromise of individuals personal safety and wellbeing if members of the public are unable to access critical fire warnings or incident information from the website during an emergency period;</li> <li>• impact on essential and/or emergency services, with a lack of capacity to operate and deliver these; and/or</li> <li>• reputational damage to the agency (CFA) if the corporate website is unavailable for a period of time during an emergency period.</li> </ul>
<p data-bbox="225 1794 363 1856"><b>Availability result</b></p>	<p data-bbox="472 1794 1310 1868">A compromise to the <b>availability</b> of the public sector information was assessed as a <b>major</b> business impact level <b>(BIL of 3)</b>.</p>

**Overall assessment result**

In this working example, the overall security value of the information was a **BIL of 3**.

This was based on the selection of the **highest BIL** from each of the three assessments (i.e. confidentiality, integrity and availability).

 <small>CONFIDENTIALITY</small>	<p><b>(BIL) of 1</b> Corresponding protective marking of <b>OFFICIAL</b> to be considered for this content</p>
 <small>INTEGRITY</small>	<p><b>(BIL) of 3</b> N.B. The outcomes of this assessment do not alter the protective marking</p>
 <small>AVAILABILITY</small>	<p><b>(BIL) of 3</b> N.B. The outcomes of this assessment do not alter the protective marking</p>

In this example, the ‘*integrity*’ and ‘*availability*’ assessment outcomes (**BILs of 3**) were higher than the ‘*confidentiality*’ (**BIL of 1**) outcome.

As there are limited confidentiality concerns with this information, the publishing team at CFA can now seek internal authorisation to publicly release this content on their website.

N.B. The protective marking of ‘**OFFICIAL**’ does not impose overly strong technical controls.

Given the **BIL of 3**, CFA should identify the associated integrity and availability risks and apply relevant controls to protect this information.

The publishing team may wish to discuss the heightened risks that they have identified during their assessment process and seek confirmation with their IT colleagues that appropriate controls have been built into the website, or identify opportunities to add extra security controls on the website, ensuring the continued integrity and availability of the material when published.

This example highlights the valuable nature of a layered assessment by helping identify where additional security measures (ICT, personnel and physical security controls) may be required to further protect the information. These security measures are beyond those informed by the protective marking of the information.

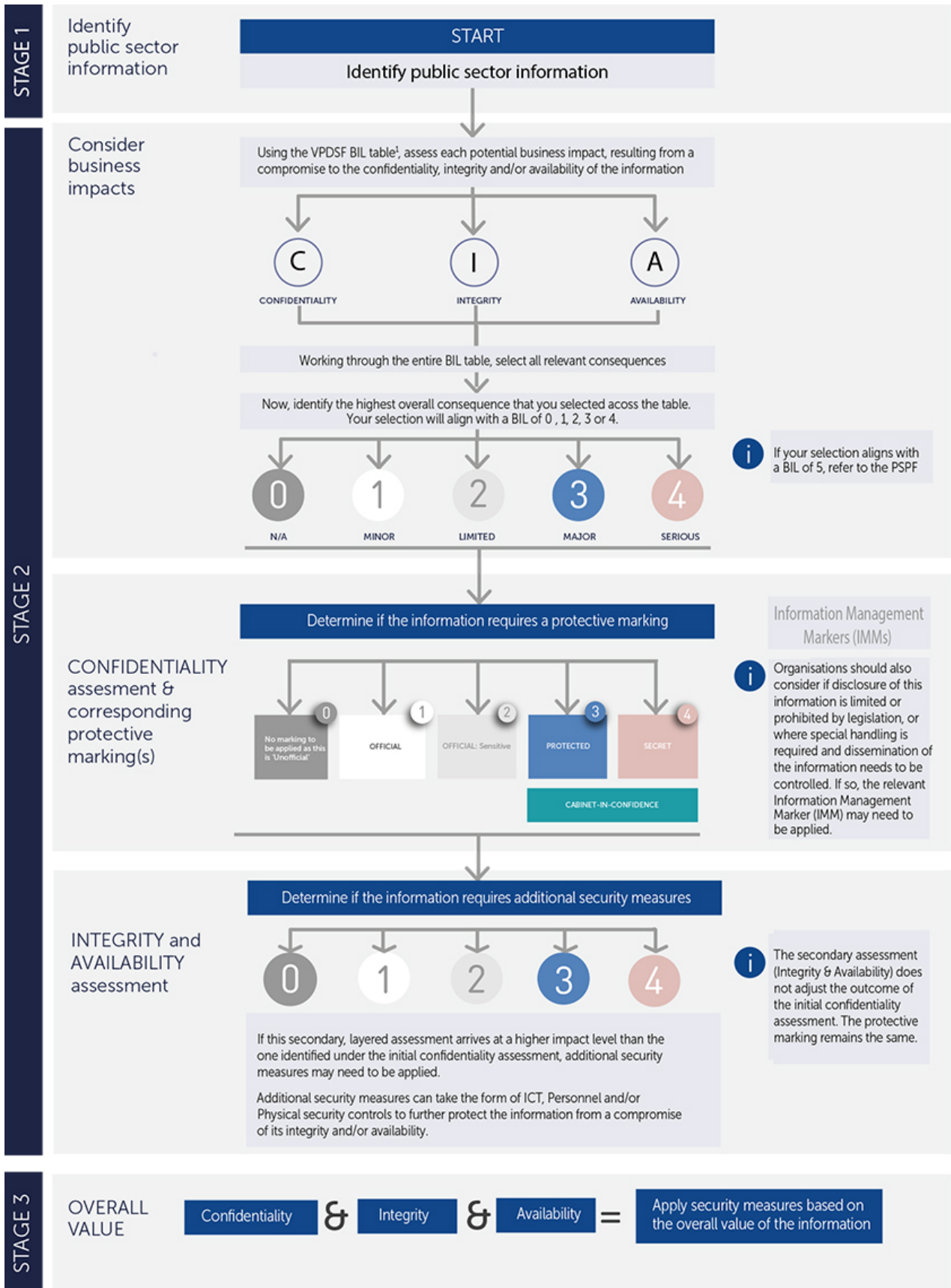
The team should also be mindful of any legislative obligations underpinning the management of the information when determining how to properly protect it and the subsequent application of information management markers.

#### 14. Information lifecycle and security value assessments

Organisations should consider the security value of public sector information across its lifecycle. The security value of the information may change due to the:

- age of the information;
- currency of the information;
- amount of information contained in a particular information asset (i.e. if content is added to or removed, the overall value of the information may change);
- aggregation of information (e.g. when data is combined with other data sets);
- information owners and owning organisations (e.g. internal organisational restructures or machinery of government activities);
- information usage (e.g. the purpose for the information collection, methods of use);
- emphasis placed on the information (i.e. no longer supporting a critical business function or activity);  
and
- internal or external circumstances that may result in a requirement to upgrade or downgrade the overall value of the information.

Appendix A – Performing an information security value assessment



## Appendix B – VPDSF Business Impact Level (BIL) Table

To download a current copy of the VPDSF BIL table, please refer to the VPDSF Resources section of the OVIC website.



### Please note:

- Harm refers to an impact on a person whereas damage refers to an impact on an asset
- For impacts of a 'National Interest' refer to the Australian Government Business Impact Levels outlined in the Commonwealth PSPF
- Protective markings only relate to confidentiality, there is no equivalent set of 'protective markings' for integrity or availability, however the business impact level table should be used to assess the impact to integrity and availability of information.