



Gov 2.0 projects in VPS: An introduction to managing risk

The support of the Department of Business and Innovation is acknowledged in allowing the adaptation of their risk management toolkit.

Contents

1	Introduction	3
	1.1 This document's purpose	3
	1.2 How to read this document	4
	1.3 Before you start	4
2	Guide to Gov 2.0 risk management	6
	2.1 How to read this section	6
	2.2 Find risks	7
	2.3 Information publication and management risks	8
	2.4 Moderation risks	9
	2.5 Resourcing risks	11
	2.6 Project management risks	12
3	Who's doing it well?	13
	3.1 Projects	13
	3.2 Documents	15
4	Gov 2.0 risks	17

1 Introduction

1.1 This document's purpose

If you're a VPS employee thinking about proposing a Gov 2.0 project, you'll need to consider a range of risks relating to Gov 2.0 projects. Gov 2.0 encompasses a number of new approaches and social media technologies (such as open collaboration, Facebook and Twitter), and there's a similarly broad range of risks to consider.

Dealing with relevant risks is a natural part of making sure your project's objectives are clear, and its design is fit for purpose.

Gov 2.0 risks are manageable, and with a bit of preparation, you will be able to propose mitigation approaches for your project's specific situation.

This document is designed to help you understand:

1. The potential risks of Gov 2.0 projects
2. How to manage these risks for a successful Gov 2.0 project
3. How to use the VPS Gov 2.0 Risk Management Plan so that you can formalise your approach to managing risks.

What this document *won't* do:

1. Provide design advice on crafting your Gov 2.0 project
2. Inform you of every single risk which is relevant to your project. Make sure you think about your own project, and what additional risks you may face.

Once you've finished this document, you will need to complete the **VPS Gov 2.0 Risk Management Plan** for your project. The term VPS when used in this document applies to the relevant department or agency within the VPS that is using this document.



The **VPS Gov 2.0 Risk Management Plan** provides further information about Gov 2.0 risks, and a structure for responding to risks, as part of appropriate risk management processes for proposed projects.

Terminology

This document uses the term **Gov 2.0** to refer to projects conducted online and characterised by interaction, collaboration and user-generated content. These projects often use **social media** tools and technologies – also commonly referred to as **Web 2.0** – to achieve their goals. **Social media** is used to refer to these technologies which may be used by the projects – and **Gov 2.0** is used to refer to the projects overall.



1.2 How to read this document

This document is split into three sections:

- [Guide to Gov 2.0 risk management](#)
Explains how to approach risks for a Gov 2.0 project, and issues that may need to be addressed. Identifies specific risks which link to the definitions in the 'Gov 2.0 risks' section.
- [Who's doing it well?](#)
Provides links to Victorian Government Gov 2.0 projects and other Gov 2.0 projects which demonstrate appropriate use of Gov 2.0 and related technologies.
- [Gov 2.0 risks](#)
Contains detailed definitions of Gov 2.0 risks, including potential consequences and links to relevant government Gov 2.0 projects and reports.

But first ...

1.3 Before you start

For a successful Gov 2.0 project, your most fundamental and important challenge is to ensure your project is well defined, and has clear objectives. Before you start thinking about the risks included in this document, make sure you have convincing answers for the questions:



Social media is an exciting new technology, and it's easy to be carried away by the enthusiasm and opportunities it offers. It's vitally important to position your business objectives at the centre of your planning, not the technology itself.

Once you are certain you have clearly defined your objectives and expectations for your project, and you are certain that social media is the right choice to achieve these objectives, it's time to consider the risks of Gov 2.0 projects, and address the relevant ones appropriately.

2 Guide to Gov 2.0 risk management

2.1 How to read this section

This section is designed to help you approach the risks and issues which may challenge your Gov 2.0 project. The risk information is presented in four categories:

- [Information publication and management](#): risks relating to the storage, secure management and publication of content for Gov 2.0 projects
- [Moderation](#): risks relating to the management and publication of user-generated content
- [Resourcing](#): risks relating to the allocation of resources and staff to Gov 2.0 projects
- [Project management](#): risks relating to the management of the project and measurement of success.

Within each of these categories, risk information is presented in the following structure:

Questions	Related risks	Why is this important?
[questions to help you think about how to address each category]	[the specific risk/s associated with each question/set of questions. The risks are linked to detailed definitions in section 4]	[specific challenges relating to the implementation of Gov 2.0 projects]

For all questions which are relevant to your project, ensure you understand why they are important, referring to the risk information in section 4 if need be. For each question, ensure it will be addressed through the planning and preparation for your project.

Gov 2.0 projects may involve any combination of:

- New or existing government websites
- Content publication on non-government sites such as YouTube
- New online applications or widgets.

Therefore, this document uses “Gov 2.0 presence” to refer to how the Gov 2.0 project exists online.

2.2 Find risks

If you've already read the VPS Gov 2.0 Risk Management Plan, you may want to quickly find the specific risks that apply to your project in this document. Consult this table to locate them in the following sections and pages.

Risk	Sections	Pages
Inappropriate choice of Gov 2.0	Before you start	4
	Project management	12
Legal liability	Information publication and management	8
	Moderation	9
Brand damage	Moderation	9
Breach of publication rights	Information publication and management	8
Breach of implicit trust	Moderation	9
Breach of confidentiality (information privacy)	Information publication and management	8
Information privacy scope	Information publication and management	8
Information quality and integrity	Information publication and management	8
Loss of control of published information	Information publication and management	8
Increased cost of service provision	Resourcing	11
Cost of information provision	Resourcing	11
Diversion from primary objectives	Project management	12
Benefits realisation	Project management	12
Business impact of dependency	Project management	12
Hijacking	Moderation	9
Authentication, identity and disclosure	Moderation	9

2.3 Information publication and management risks

These questions relate to the storage, secure management, and publication of government content for Gov 2.0 projects. This content may be text, images, video or audio, and may be published on a Gov 2.0 presence hosted on a government website, or hosted on an external website (e.g. a video published on YouTube).

Questions	Risks to consider	Why is this important?
<input type="checkbox"/> How will you determine what government information can be published on the Gov 2.0 presence? (e.g. with regards to confidentiality, copyright/digital rights) <input type="checkbox"/> How will you manage security for the information you plan to publish? <input type="checkbox"/> How can you make sure VPS employees who will use the Gov 2.0 presence will understand and know how to use all related information security tools? <input type="checkbox"/> How can you customise the publication process to add any necessary security and quality control measures?	Legal liability Information privacy scope Information quality and integrity Breach of publication rights Breach of confidentiality (information privacy)	<p>Gov 2.0 projects need to provide adequate control over the information that is published, and how it can be consumed or shared.</p> <p>Existing tools and processes to manage information security will need to be reviewed, updated if required, and reinforced amongst VPS and Government users of the online presence. These tools and processes include:</p> <ol style="list-style-type: none"> 1. Confidentiality classifications 2. Information handling procedures.
<input type="checkbox"/> How will you manage content over its lifecycle, and do you have access to all the tools you need? <input type="checkbox"/> Have you considered whether you will be able to re-use existing online content for the Gov 2.0 presence? <input type="checkbox"/> How can you make sure VPS employees who will use the Gov 2.0 presence will understand and know how to use the content management tools?	Loss of control of published information	<p>Gov 2.0 projects need to consider content lifecycle management controls to identify information with time-sensitive publication needs, and manage it accordingly. This may include a review and update of existing processes.</p> <p>Existing tools and processes to manage publication, maintenance and retirement will need to be reinforced amongst VPS and Government employees who may publish content.</p>

2.4 Moderation risks

These questions relate to the management and publication of user-contributed content on Gov 2.0 presences. This content may be text, images, video or audio, and may be submitted for publication in response to existing content (e.g. a comment on a blog post), or may be standalone content (e.g. a video submission for a competition).

These questions are applicable to any Gov 2.0 project which allows users to provide content for publication on the presence.

Questions	Risks to consider	Why is this important?
<input type="checkbox"/> How will you moderate user-contributed content (e.g. comments, videos, audio), either before or after publication?	Legal liability Brand damage Hijacking	Gov 2.0 projects need moderation tools so VPS can exercise control over user-generated content, before or after publication.
<input type="checkbox"/> What is your process for responding to negative content published by users?	Brand damage	When removal of negative user-generated content is not an option, Gov 2.0 projects need an approach for engaging in dialogue to respond to this content. Even when content can be removed, a dialogue may still be required.
<input type="checkbox"/> How will you closely monitor user input for duplicate posting, vote rigging, and other ways of influencing discussion? <input type="checkbox"/> How will you manage a situation where users intentionally try to influence discussion or content?	Hijacking	Gov 2.0 projects need to monitor usage and content to identify any patterns of behaviour which indicate an intentional effort to influence discussion or content. They need a clear approach for handling such a situation.
<input type="checkbox"/> How will you set expectations among users for what is likely to happen as a result of the project, forum or collaboration? <input type="checkbox"/> How will you require users to agree to the way their contributions will be used?	Breach of implicit trust	Gov 2.0 projects need to clearly set expectations among users about whether their input will definitely lead to any specific action. If the content will be republished on a different platform (e.g. print), permission will need to be obtained.

Questions	Risks to consider	Why is this important?
<input type="checkbox"/> What is the minimum amount of personal data your users will be willing to provide, to deliver meaningful results? <input type="checkbox"/> What behaviour will you require users to agree to before they may participate?	Authentication, identity and disclosure	Gov 2.0 projects need to strike a balance between requiring too much personal information and delivering meaningful results. A Gov 2.0 presence should be clear about the behaviour expected from users, and seek their agreement when they sign up.

2.5 Resourcing risks

These questions relate to the allocation of resources and staff to Gov 2.0 projects, and the management of costs for the project.

Questions	Risks to consider	Why is this important?
<input type="checkbox"/> What resources and skills will be needed for your project, and what will be the associated costs (both one-off and ongoing)? <input type="checkbox"/> Which employees will be involved, and what will be their roles and responsibilities? <input type="checkbox"/> Will external organisations be involved, and what will be their roles and responsibilities? <input type="checkbox"/> What Central Web Team support will you need to implement and administer the Gov 2.0 presence?	Increased cost of service provision	Gov 2.0 projects need clear definition of resourcing and skills requirements, and accurate assessment of associated costs.
<input type="checkbox"/> What resources and skills will be needed for content preparation, both at launch and ongoing, and what will be the associated costs? <input type="checkbox"/> What will be the ongoing resources and skills needed, and costs for maintenance and management of the project? <input type="checkbox"/> What obligations and costs will need to be met in decommissioning (or migrating) the Gov 2.0 presence?	Cost of information provision	Gov 2.0 projects need clear definition of resourcing and skills requirements for content preparation, and associated costs, and must secure these resources as long as the presence operates.

2.6 Project management risks

These questions relate to the management of a Gov 2.0 project, and the methods for measuring the success of the project.

Questions	Risks to consider	Why is this important?
<input type="checkbox"/> What are the business objectives of your project, and how will you measure the success of these objectives? <input type="checkbox"/> If tools to measure these objectives aren't already available, what new tools will need to be developed or obtained?	Benefits realisation Inappropriate choice of Gov 2.0	<p>Measuring success of Gov 2.0 projects can be difficult, and adequate preparation and research must be conducted into how to do so.</p> <p>Tools and techniques need to be available to measure, analyse and report on business objectives.</p>
<input type="checkbox"/> How can you make sure your project doesn't compromise service delivery – either on the Gov 2.0 presence, or on a different medium such as a call centre? <input type="checkbox"/> How can necessary resources and skills be organised for your project without diverting resources from existing service delivery?	Diversion from primary objectives	<p>Gov 2.0 projects should not interfere with the delivery of existing services, either through their resource requirements or through their technical processes.</p>
<input type="checkbox"/> What other projects or activities are dependent on your project's timeline? <input type="checkbox"/> How will you be able to manage these dependencies?	Business impact of dependency	<p>Gov 2.0 projects need a clear approach to managing dependencies with other projects or activities.</p>

3 Who's doing it well?

There are countless examples of how governments can use Gov 2.0 well, some of which are included here. There are also numerous documents purporting to educate you on the perfect way of getting involved with Gov 2.0. We've selected some of the best, and included them here, too.

3.1 Projects

3.1.1 Victorian Government projects

Organisation	Project	Social media type	How does it succeed?	Link
Small Business Victoria	I am a business owner in Victoria, Australia	Facebook	Visiting experts answer members' questions during virtual question and answer sessions. Confidential, government information is not published on Facebook.	http://www.facebook.com/group.php?gid=114352295710
Skills Victoria	Nova's Got Skills	Twitter	Leveraged the Nova radio brand, already familiar to target audience, to promote Skills messages and receive hundreds of competition entries.	http://www.skills.vic.gov.au/events/novas-got-skills-campaign
Premier of Victoria	Got an idea?	Ideation forum	Moderates comments within business hours, and is clear about the possibility for delays. Requires registration to vote or submit idea, reducing risk of 'gaming' the results.	http://www.premier.vic.gov.au/share-your-ideas.html
Premier of Victoria	YouTube Question Time	YouTube	Users are alerted to how their input will be used, when to expect responses, and the kind of response that they will receive.	http://www.youtube.com/user/premierofvictoria
Premier of Victoria	App My State	Ideation and open data	Generates interest around the move to open government data, encourages citizens to submit ideas and generate opportunities for use of data.	http://www.premier.vic.gov.au/app-my-state.html

Organisation	Project	Social media type	How does it succeed?	Link
National Gallery of Victoria		Facebook	Posts updates about events at the Gallery, displays many photo galleries of related images, and is quick to respond to posts and questions.	http://www.facebook.com/pages/Melbourne-Australia/National-Gallery-of-Victoria/177176991162
Film Victoria		Twitter	Short updates with links to longer articles and film events. Posts consistently on-topic content with links to relevant information for its readers.	http://twitter.com/filmvictoria

3.1.2 Other projects

Organisation	Project	Social media type	How does it succeed?	Link
Center for Disease Control – USA		Facebook	Frequent posting about health issues, CDC offerings, and social media tools and widgets – appealing to a wide range of audience needs. Clear disclaimer regarding not being responsible for comments and images posted by 3 rd parties.	http://www.facebook.com/CDC
My Society – UK	Write To Them	Mash-up	Provides simple and easy access to government through a postcode search to find a representative, and a pre-built form for contacting them.	http://www.writetothem.com
My Society – UK	Fix My Street	Mash-up	Provides simple and easy access to request government to perform repairs.	http://www.fixmystreet.com
My Society – UK	They Work For You	Mash-up	Provides simple and easy access to government information by collating and displaying all government activity for the representative for a user's location, and providing options to contact them.	http://www.theyworkforyou.com

Organisation	Project	Social media type	How does it succeed?	Link
Open Australia		Mash-up	Provides simple and easy access to government information by collating and displaying all government activity for the representative for a user's location, and providing options to contact them.	http://www.openaustralia.org
Future Melbourne		Collaboration	Generated high-quality input from participants over a 4 week period, with no spam or off-topic input. Requirement for registration created a barrier to casual users with malicious intent.	http://www.futuremelbourne.com.au
WebCitizen – Brazil	Vote Na Web	Mash-up / Collaboration	Encourages engagement in democratic process by allowing users to vote on topics being considered by the government.	http://www.votenaweb.com.br

3.2 Documents

Title	Author/Publisher	How can it help?	Link
Project report: "Adoption, Barriers, Best Practice and Recommendations of Gov 2.0 in Government"	Government 2.0 Taskforce, Australian Government	Extremely detailed information about management of barriers to engaging with Gov 2.0, can provide advice and inspiration.	http://gov2.net.au/files/2009/12/Project-2-and-3-Final-Report.doc
Engage: Getting on with Government 2.0	Government 2.0 Taskforce, Australian Government	Explains Gov 2.0 in great detail, with advice on both high level philosophical issues and finer points of implementation.	http://www.finance.gov.au/publications/gov20taskforcereport/index.html
Response to "Engage"	Australian Government	Explains Federal Government's approach to Gov 2.0, including recommendations for government employees' online behaviour and licensing of government material online.	http://www.finance.gov.au/publications/govresponse20report

Title	Author/Publisher	How can it help?	Link
VPS department or agency website minimum requirements and best practice	VPS department or agency	Internal document available on the intranet. Useful ideas for how to manage social media and the processes you may need to engage with or replicate for your project.	[Internal document]
Future Melbourne Wiki Post Implementation Review	City of Melbourne & Collabforge	Documents learnings and insight gained from a successful collaborative project.	http://www.futuremelbourne.com.au/wiki/pub/FMPlan/WebHome/Future_Melbourne_Wiki_Post_Implementation_.pdf

4 Gov 2.0 risks

This table defines in detail some potential risks associated with Gov 2.0 projects, categorised by broad risk type, with indicative consequences presented as well. You will find these risks within the VPS Gov 2.0 Risk Management Plan, which you will need to complete for your project.

Category	Risk	Brief description	Full definition	Consequences
Strategic	Inappropriate choice of social media	Government chooses to use social media for engagement or collaboration where its use will not meet business objectives.	Social media is an exciting new development in online technologies, and has become extremely popular among members of the public. It is tempting to use social media for projects because of the general attractiveness and popularity of the technology, even if it's not actually the most appropriate solution for a business problem. If the solution is chosen before the problem is considered, business objectives can be difficult to meet, or even define. Any Gov 2.0 project will need to ensure the technology chosen is appropriate for the business problem being addressed.	Business objectives cannot be met and initiative fails. Increased likelihood of all other Gov 2.0 risks listed below.
Reputation	Legal liability	A citizen holds government liable for damaging consequences of information provided via a Gov 2.0 service.	VPS will be held responsible for any content which is published on an online presence it manages, whether it's written by a VPS employee or a member of the public. If a reader chooses to take legal action regarding content, VPS is therefore likely to be the target. Any Gov 2.0 project will need to minimise the risk of legal action being taken against the VPS.	Legal action against government.

Category	Risk	Brief description	Full definition	Consequences
Reputation	Brand damage	A user contributes content that damages government or ministerial reputation (key stakeholder perception of Departmental credibility).	Allowing users to publish content on an online presence which VPS manages creates the opportunity for the users to publish content which damages government or ministerial reputation. Insufficient or inefficient tools and processes for managing the presence increases the risk of this occurring. Any Gov 2.0 project will need to minimise the risk of damaging content being published on the online presence.	Damage to government reputation and public perception of integrity.
Reputation	Breach of publication rights	A public servant publishes content (or digital assets) that infringes copyright (or agreed/licensed digital rights).	Social media presences often provide easy, straightforward ways to publish content online, without requiring the publisher to consider whether the publication infringes copyright or digital rights restrictions on that content. Any Gov 2.0 project will need to minimise the risk of content being published in a method that infringes copyright or digital rights.	Legal action against government by content owner. Damage to government reputation and public perception of integrity.
Reputation	Breach of implicit trust	A government decision is contrary to public feedback requested and received by government on a Gov 2.0 forum.	Gov 2.0 presences designed to elicit opinions and feedback from members of the public serve as a communication pathway from the public to the government. When action taken by Government, subsequent to receiving opinions and feedback from the public, differs from the action the public wanted the Government to take, the public can cast doubt on the Gov 2.0 presence. They may see it as a tokenistic approach lacking in any intent to follow through on feedback received, and assume that the Government was either not listening to the channel, or, listening but not caring. Any Gov 2.0 project will need to minimise the risk of setting up expectations among its users that their input will definitely lead to any specific action.	Damage to government reputation and public perception of integrity and care for public.

Category	Risk	Brief description	Full definition	Consequences
Reputation	Breach of confidentiality (information privacy)	A government employee inadvertently releases confidential or private information on a Gov 2.0 channel.	The inherently public and networked nature of Gov 2.0 presences means that information in electronic form can easily be shared, published and publicised . Confidential or private information is at particular risk of being shared, and then republished on inappropriate sites. Any Gov 2.0 project will need to minimise such a risk, through clear processes for handling and publishing information, which should also be clearly labelled as being confidential or private.	Legal action against government by subject(s) of confidential information. Damage to government reputation and public perception of integrity.
Reputation	Information privacy scope	A government employee publishes information which gains unintended uses as a result of broader access.	The publication by VPS employees of government information in an online presence creates the opportunity for that information to be used by other people and organisations in ways not sanctioned by VPS. Due to the permanence and replicability of content published online, it is easy for a reader to use or republish content without gaining VPS's permission first. Any Gov 2.0 project will need to minimise the risk of information becoming at risk of such unintended re-use.	Damage to government reputation and public perception of integrity.
Reputation	Information quality and integrity	A government employee publishes information that is inaccurate, has been superseded, or lacks integrity or quality.	Government information published on an online presence needs to be accurate, up-to-date and of sufficient quality to effectively represent Government and VPS in a positive fashion. Information which does not meet these requirements can damage the Government and VPS's reputation by implying a lack of effective data management. Any Gov 2.0 project will need to minimise the risk of negative presentations of Government and VPS through information of a substandard quality.	Damage to government reputation and public perception of integrity.

Category	Risk	Brief description	Full definition	Consequences
Reputation	Loss of control of published information	Government publishes information on a Gov 2.0 service and then finds it cannot be deleted or withdrawn.	Information published on a social media platform owned by a non-Government entity, such as Facebook or LinkedIn, is ultimately bound by the technical or legal limitations of that platform. If content published on such a platform cannot be deleted, edited or withdrawn, managing mis-publication becomes difficult if not impossible to perform. Any Gov 2.0 project will need to minimise the risk of information needing to be deleted or edited on a platform which does not support this.	Damage to government reputation and public perception of integrity.
Cost	Increased cost of service provision	Adoption of Gov 2.0 service delivery or service augmentation increases service delivery costs (due to additional resourcing, staff training and additional tool use, compliance, monitoring, record-keeping, auditing, increased enquiry/complaint volumes or other reasons).	Gov 2.0 project requirements can lead to additions and/or alterations to existing service delivery methods and processes. As Gov 2.0 requirements are not yet firmly embedded in departmental or governmental processes, the increased costs which can accompany the fulfilment of these requirements can be unexpected, and lead to negative consequences for a project and for Gov 2.0 support in general within VPS and Government. Any Gov 2.0 project will need to minimise the risk that costs related to service provision are not recognised and managed responsibly.	Service delivery cost increases.

Category	Risk	Brief description	Full definition	Consequences
Cost	Cost of information provision	Provision of new or additional information increases costs (due to formatting, reviewing, approval, or other resourcing factors).	Preparation of content for publication on Gov 2.0 online presences can include different tasks and responsibilities from preparation for publication on a traditional channel. A 'one-size-fits-all' approach can lead to missed deadlines and inappropriate responses, while provision of appropriate processes can result in unforeseen additional expenses. Any Gov 2.0 project will need to minimise the risk that costs related to content preparation are recognised and managed responsibly.	Service delivery cost increases.
Target performance	Diversion from primary objectives	A business unit's adoption of a Gov 2.0 service causes primary service delivery objectives to be compromised (through diversion of resources, loss of control of resources, engagement in low-priority issues, online participation, moderation, etc.)	Gov 2.0 projects bring a variety of challenges and standard operating requirements that VPS will need to respond to appropriately, without becoming diverted from the primary, existing objectives of service delivery. Unrealistic expectations, a lack of preparation, and a lack of skills in responding to these challenges and requirements can lead directly to resources being diverted on an <i>ad hoc</i> basis, with little long-term understanding of, or planning for, the consequences. Any Gov 2.0 project will need to minimise the risk that foreseeable challenges and requirements are not managed in an appropriate timeframe.	Primary (or other) service delivery objectives are compromised (quality, responsiveness).

Category	Risk	Brief description	Full definition	Consequences
Target performance	Benefits realisation	A business unit embarks on a Gov 2.0 project but does not (or cannot) define measurable objectives (KPIs).	As Gov 2.0 is not embedded yet in departmental and government processes, Gov 2.0 projects are testbeds where expectations and fears are tried and reported back to decision makers. Without clear evidence of results, success or failure can be difficult to identify, and without existing, tried and true KPIs available for ready integration into a Gov 2.0 project, even having results available may not lead to a clear identification of success or failure. Any Gov 2.0 project will need to minimise the risk that goals, and therefore success, are not identified.	There is no accounting for cost and effort, or return on investment.
Schedule	Business impact of dependency	Risk that a Gov 2.0 service will cause delivery slippage of a related or dependent project.	Due to the social, partially uncontrollable nature of Gov 2.0 online presences, it can be hard to predict whether project achievements will occur within an expected timeline. Projects or tasks which are dependent upon such an achievement can therefore experience a related slippage in timelines. Any Gov 2.0 project will need to minimise the risk that dependent projects or tasks experience such a slippage.	Slippage of related or dependent project(s).

Category	Risk	Brief description	Full definition	Consequences
Fit for purpose	Hijacking	Risk that a Gov 2.0 service that is open to the public will be hijacked by individuals, industry lobby groups, or special interest groups.	As Gov 2.0 projects are by nature public, social online presences, and as VPS's intended audience will often be members of the public, individuals or organisations with specific or ulterior motives can easily gain access to these presences. It is important to ensure that such users are unable to intentionally influence discussion or content in a direction which defeats the purpose of the project, and which causes additional difficulties and negative consequences for the VPS or Government. Any Gov 2.0 project will need to minimise the risk that users of the online presence will be able to influence discussion or content in such a way.	Distortion of perspective, skewed results, misrepresentation of public opinion.
Fit for purpose	Authentication, identity and disclosure	Risk that the anonymity of the service recipient will compromise service delivery.	When gathering opinions and input from users on a Gov 2.0 presence, it's important to know who you're gathering information from. Without enough identifying information, the data can end up being meaningless. However, Gov 2.0 users are often reticent to hand over personal information, and asking them to hand over too much can lead to them handing over no information, and no opinions or input. Finding the balance can be hard, but is necessary if you want your project to deliver adequate, meaningful results. Any Gov 2.0 project will need to find this balance.	Insufficient project results, or not sufficiently meaningful.