Accounting and Management Information Systems
Vol. 10, No. 4, pp. 495–515, 2011

USING CONTROL FRAMEWORKS TO MAP RISKS IN WEB 2.0 APPLICATIONS

Riaan J. RUDMAN[1]
Department of Accounting, Stellenbosch University, South-Africa

ABSTRACT

Web 2.0 applications are continuously moving into the corporate mainstream. Each new development brings its own threats or new ways to deliver old attacks. The objective of this study is to develop a framework to identify the security issues an organisation is exposed to through Web 2.0 applications, with specific focus on unauthorised access. An extensive literature review was performed to obtain an understanding of the technologies driving Web 2.0 applications. Thereafter, the technologies were mapped against Control Objectives for Information and related Technology and Trust Service Principles and Criteria and associated control objectives relating to security risks. These objectives were used to develop a framework which can be used to identify risks and formulate appropriate internal control measures in any organisation using Web 2.0 applications. Every organisation, technology and application is unique and the safeguards depend on the nature of the organisation, information at stake, degree of vulnerability and risks. A comprehensive security program should include a multi-layer approach comprising of a control framework, combined with a control model considering the control processes in order to identify the appropriate control techniques.

Web 2.0, Security risks, Control framework, Control Objectives for Information and related Technology (CobiT), Trust Service Principles and Criteria

INTRODUCTION

Technological advances transformed the Internet into a marketplace of services. A recent trend in information technology is business-to-business collaboration, where business functionality is supported through virtual applications (Coetzee & Eloff,

[1] *Correspondence address:* Riaan Rudman, Stellenbosch University; tel. +27 (0) 72-1888-022; email address: RJRudman@sun.ac.za

2005). This includes Web 2.0 applications. These technologies have moved into the corporate mainstream. This trend is expected to continue (Metz, 2007, Valdes, 2008) and is driven by the new generation of Internet users entering the workforce and bringing with them the familiarity of social computing tools (Ghandi, 2008). As users become more comfortable with technological advances in their personal lives, they also demand this in their professional lives (Bradley, 2007). They have different views on work habits, data access and multi-tasking and may experience a conflict within established workplace environments and policies where connectivity is tightly controlled, resulting in that the control assumptions on which most control frameworks are based, are no longer relevant (Cavoukian & Tapscott, 2006). This resulted in traditional control techniques being less effective (D'Agostino, 2006). Consequently, each new development of the Internet brings its own threats or new ways to deliver old attacks (Georgia Tech Information Security Centre [GTISC], 2008). Consequently, a new way of identifying and evaluating risks needs to be developed in order for controls to be developed to mitigate the risks. This leads to the research question: Which framework can be used to identify the intrusion risks that an organisation is exposed to when Web 2.0 applications are used and can this framework be used to identify risks and recommend controls that should be present to mitigate these risks?

1. RESEARCH OBJECTIVE AND METHODOLOGY

The objective of this study is to develop a framework to identify and manage the security issues an organisation is exposed to that arise from Web 2.0 applications, with specific focus on significant intrusion risks. The research study focuses on developing a framework that can be used to identify the significant risks arising as a direct consequence of end-users using Web 2.0 applications and not on all the risks prevalent to the Internet or general e-commerce. It is not the purpose of this study to define or debate Web 2.0, but rather to investigate Web 2.0 in general terms; accordingly, technical discussions on the technologies underlying Web 2.0 are not provided.

Obtaining an understanding of Web 2.0 and Web 2.0 security is important, as Web 2.0 is a new, poorly understood technology and with the growing mobility of users and wireless technology, the potential surface area of attack increases (D'Agostino, 2006) and should be managed. This study will provide organisations, Information Technology (IT) professionals and internal and external auditors with a framework to identify and manage the 'new' risks that arise in this new online environment.

In order to identify the security risks and develop a framework of internal controls over Web 2.0 applications, it was first necessary to obtain an understanding of the technologies driving Web 2.0 applications by performing an extensive literature review. Thereafter, an appropriate control framework and model to be used to identify the risk applicable to Web 2.0 technologies had to be selected. The technology was mapped against the selected framework and model and associated control objectives relating to security risks (specifically to unauthorised access). These objectives were used to identify relevant risks. The impact of each risk was evaluated and suitable internal control measures formulated. The objectives, risks and controls form the framework.

Section 2 describes Web 2.0 and related technologies. Section 3 presents an overview of prior research conducted. Section 4 includes a discussion on the frameworks selected, and highlights the importance thereof. Section 5 documents the framework applied to Web 2.0 technologies, briefly outlining the risks and related safeguards. The study is concluded in Section 6 and contains suggestions for future research opportunities.

2. WEB 2.0

The term 'Web 2.0' is not well defined (Radcliff, 2007). According to Wikipedia (2008), an online encyclopaedia, the publicly accepted definition for Web 2.0 is *"a perceived second generation of web-based communities and host servers that facilitate collaboration and sharing between users; referring to a change in the way that the platform is used.*" It is the evolution of the browser from a static request-response interface to a dynamic, asynchronous interface with Web 2.0 providing the architecture of participation by users with a rich user interface that allows them to create, collaborate and share information on a real-time basis, creating an idea of a community of collective intelligence. This participation enhances the accessibility of information and in doing so, distributes control to end-users (Rudman, 2007a).

Web 2.0 can be classified in terms of its (i) components, (ii) technology and (iii) programming. The key features of Web 2.0 sites can be summarised as having the following three components:

- **Community and social:** software that permits users to study, change and improve content or software (or source-code) and to simultaneously redistribute and re-use it in modified form. This component considers the dynamics around social networks, communities and personal content publishing tools that facilitate sharing and collaboration.
- **Technology and architecture:** web-based applications with a rich interface that run in a web browser and do not require specific software installation, a specific device or platform (including mobile devices), but still have the features of traditional applications.
- **Business and process:** resources on a network made available as independent services that can be accessed without knowledge of their underlying platform implementation. Software is being delivered as a service rather than an installed product, freeing users from a specific platform or operating system, thereby creating new business models (Smith 2008).

Web 2.0 applications are based on four broad types of technologies as presented in Table 1:

Table 1. **Types of Web 2.0 technologies**

Technology	Examples of technology
1. **Publication**: Blogs and Wikis which can be edited and contribute content by various users in real-time.	Weblogs (blogs), wikis, user generated media
2. **Syndication**: allows for the sharing, consolidation and sourcing of information from various sources.	Really Simple Syndication (RSS) or newsfeeds, social tagging or bookmarking, folksonomies
3. **Collaboration**: users can create communities to collaborate or use tools to collaborate on projects.	Social networking, peer-to-peer networking, web application program interfaces (APIs)
4. **Recombination**: Flashbased players, podcasts *et cetera* are easy to create and can be used for various purposes.	Podcasts, mash-ups

It is also argued that because a website is built using a certain technology or programming such as AJAX, Flash, XAML, REST, XML, JSON Active-X plug-ins in its interface, it is a Web 2.0 application. This is another form of classification.

The debate around the questions: '*What is Web 2.0?*' and '*How to classify Web 2.0?*' continues. Web 2.0 as a field is growing, with related concepts such as Enterprise 2.0 (Cavoukian & Tapscott, 2006) also being explored and researched.

3. PRIOR RESEARCH STUDIES AND HISTORIC REVIEW

The majority of research relating to Web 2.0 has been conducted by private organisations such as *inter alia* Gartner, Clearswift, PEW/Internet & American Life Project and KPMG, with limited academic peer-reviewed research being performed (Shin, 2008). Initially, research focused on understanding the technology, its benefits, uses in a business environment and potential challenges (Matuszak, 2007; Clearswift, 2007a, b). Other research studies focused on the areas of privacy (Cavoukian & Tapscott, 2006), collaboration (Lee & Lan, 2007), usage and user behaviour patterns (Horrigan, 2007; Lenhart & Madden, 2007; Shin, 2008). As the popularity of Web 2.0 services such as Facebook, Youtube, Wikipedia *et cetera* grew, the popular media published various articles on security risks relating to Web 2.0 services, focusing mainly on business risks (D'Agostino, 2006; Fanning, 2007; Mitchell, 2007*)*. Various attempts have been made to develop an organisational framework to help businesses to understand and address both Web 2.0 risks and generate business value for enterprises using Web 2.0 applications. The most widely used frameworks were developed by Dawson (2007, 2008).

An international academic study by Bonatti and Samarati (2002) and later South African studies by Coetzee and Eloff (2005, 2007) attempted to develop access control frameworks for the Internet. Ratnasigam (2007) developed a risk-control framework for an e-market place.

The majority of research have focused, either on the technology and associated risks, or on a framework to control Internet users. A study, which specifically considers the incremental risk arising from Web 2.0 technologies and the creation of a comprehensive control framework to mitigate the risk of unauthorised access, has not been conducted.

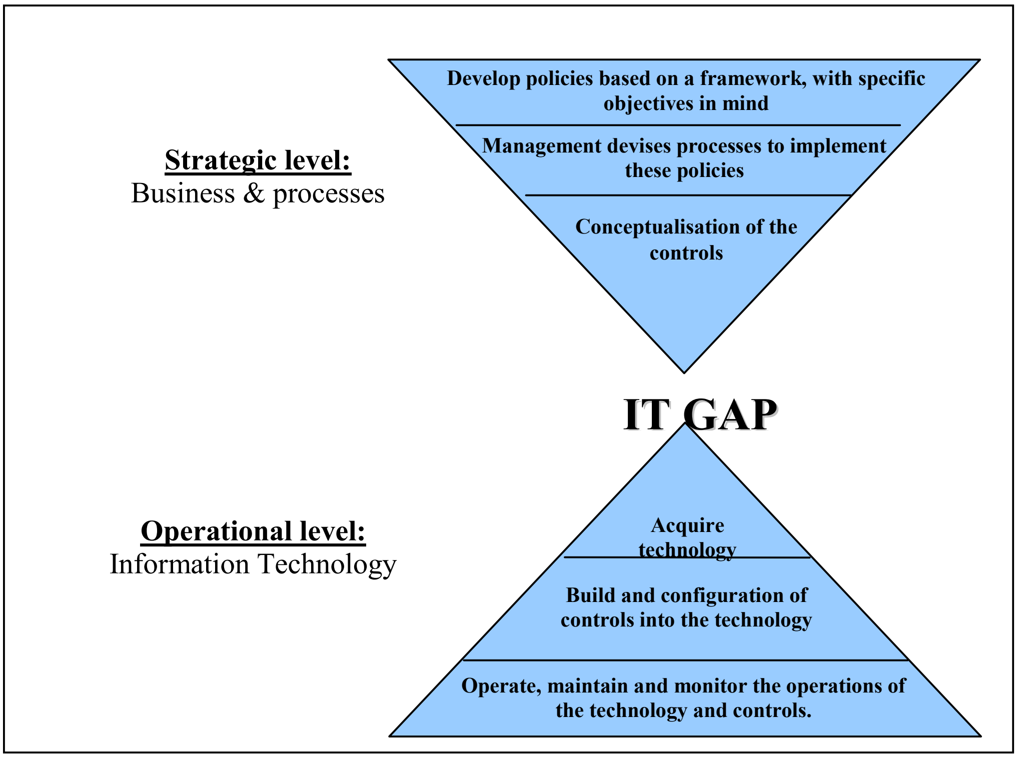
4. RISK AND CONTROL FRAMEWORK

In order to mitigate security risks, internal controls should be implemented at different levels. The Committee of Sponsoring Organisations of the Treadway Commission (COSO) (1992) defines ‘internal control’ as a process effected by an entity’s Board of Directors, management and other personnel and is designed to provide reasonable assurance regarding the achievement of objectives in the categories of effectiveness and efficiency of operations, the reliability of financial reporting and compliance with applicable laws and regulations. After identifying business objectives and associated risks, the existing controls to manage the risks should be identified and evaluated. In order to identify the risks, a proper control framework of generally accepted control practices is needed as a benchmark. These control techniques (i.e. controls) depend on the context created by the environment. However, implementing these control techniques on their own is merely *ad hoc*, if not linked to a proper control framework (providing insight into managing the system, its controls and risk effectively) or model (focusing on the design, implementation and maintenance controls).

Control techniques are implemented by IT professionals, whereas management implements a control framework and models. This creates a problem, as management does not understand the control techniques and technology, whereas IT professionals do neither understand the model, nor the framework (commonly referred to as the IT-gap as depicted in figure 1). It is this *ad hoc* implementation of controls and gap in frame of reference that creates weaknesses in any system. Risks and weaknesses are not introduced into a system because there are neither any policies and procedures nor because controls are not implemented but these rather exist as management and technical policies and procedures do not merge into one risk management unit. This research attempts to do this.

Control Objectives for Information and related Technology (CobiT) was selected as a control framework because it has been successful at a high level in addressing the security risks posed by unauthorised entry. Trust Service Principles and Criteria (Trust Services’ criteria) were used as it provided assurance over e-commerce and other related processes (Lamprecht, 2004). Both frameworks are also internationally accepted as best practices benchmarks, supported by various professional organisations (IT Governance Institute, 2006). Other frameworks and models (including ISO/ISE 17799, which specifically deals with security controls) were considered, but were not selected given the nature and characteristics of Web 2.0 applications discussed in Section 0, being e-commerce and web application based.

Figure 1. **IT Gap**


Strategic level:
Business & processes
Develop policies based on a framework, with specific objectives in mind
Management devises processes to implement these policies
Conceptualisation of the controls
IT GAP
Operational level:
Information Technology
Acquire technology
Build and configuration of controls into the technology
Operate, maintain and monitor the operations of the technology and controls.

4.1 Control framework

A control framework serves as a guideline for management to give insight into managing its systems, business risks and internal controls effectively such as the CobiT framework of the Information System Audit and Control Association and the IT Governance Institute. CobiT is used as a set of generally accepted best practices framework to assist in developing appropriate IT governance and controls and assurance in a company that links information technology to business requirements and related resources. It provides tools in the form of high level objectives, to assess and measure the performance of IT processes. Its purpose is to create generally accepted IT control objectives for day-to-day use. It provides an adaptive benchmark that sets out the objectives to be achieved by each process. It attempts to bridge the gap between business risk, control needs and technical issues. It aids management in defining IT strategies and architecture, in acquiring the necessary skills, software and hardware to execute the strategy, ensuring continuous service and evaluating the performance of the IT system (CobiT Steering Committee [CobiT], 2007).

This study uses the CobiT framework, which consists of three main parts: (i) the control framework, (ii) management guidelines and (iii) implementation toolset. The CobiT framework covers the following four domains:

- **Plan and organise (PO)**: which highlights the organisational and infrastructural form.
- **Acquire and implement (AI)**: which identifies IT requirements and acquisition and implementation of information technology within the company's current business processes. It also addresses the maintenance plan.
- **Deliver and support (DS)**: which focuses on the delivery aspects of the information technology, including the support processes as well as security issues and training.
- **Monitor and evaluate (ME)**: which covers a company's strategy in assessing the needs of the company, whether objectives are met and whether the company complies with the regulatory requirements.

Control is approached by identifying information required to support the business objectives. Information is then the result of the combined application of IT-related resources that need to be managed by IT processes. Each domain summarises several processes, linking each process to a control objective that can be used to design an appropriate control, activity or task (also known as information criteria). These can also be used to evaluate the impact on the business and IT resources. Each process is evaluated, the risks are identified, evaluated and the impact and relevance to the information criteria considered. This assists to identify the important/risk areas. The objective is that, if these processes are properly managed, information technology will be governed effectively (CobiT, 2007).

The framework above was applied to Web 2.0 technology. An extract of the worksheet used is presented in figure 2.

4.2 Control model

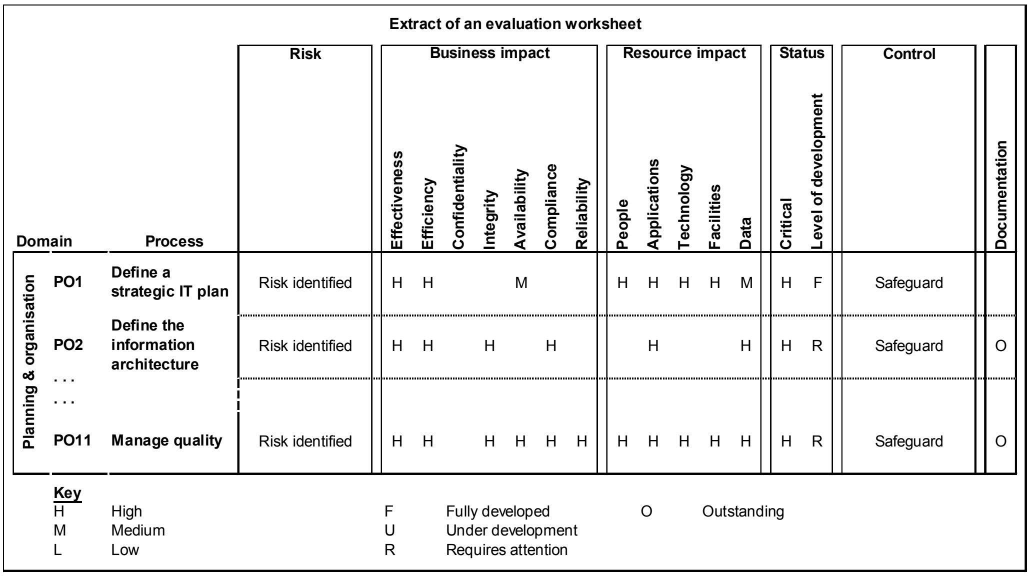
The American Institute of Certified Public Accountants, Inc. (AICPA) and Canadian Institute of Chartered Accountants (CICA) Trust Services' criteria and Illustration present a common framework with a set of core principles, criteria and illustrative controls to address risks. The Trust Services' criteria is a benchmark used to measure compliance of an e-commerce system to achieve the objectives of security, availability, processing integrity, online privacy and confidentiality. The control model focuses on the design, implementation and maintenance of risk management by identifying application-centred control objectives and a set of minimum control standards. This is also one of the reasons for selecting the model for the research. This is done through the application of control techniques.

The Trust Services' criteria are organised into four broad areas:

- **Policies**: The entity must define and document its policies relevant to a particular principle.
- **Communications**: The entity must communicate its policy to all authorised users.
- **Procedures**: Procedures should be implemented to achieve the objectives.
- **Monitoring**: A system must be implemented to monitor the compliance with these policies (AICPA/CICA, 2003).

A similar process and worksheet was used to apply Trust services' criteria as that detailed in figure 2.

Figure 2. **Extract of an evaluation worksheet used to apply CobiT**



Extract of an evaluation worksheet

			Risk	Business impact							Resource impact					Status		Control	
Domain		Process		Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	People	Applications	Technology	Facilities	Data	Critical	Level of development		Documentation
Planning & organisation	PO1	Define a strategic IT plan	Risk identified	H	H			M			H	H	H	H	M	H	F	Safeguard	
	PO2	Define the information architecture	Risk identified	H	H		H		H			H			H	H	R	Safeguard	O
	. . . . . .																		
	PO11	Manage quality	Risk identified	H	H		H	H	H	H	H	H	H	H	H	H	R	Safeguard	O

Key

H	High	F	Fully developed	O	Outstanding
M	Medium	U	Under development		
L	Low	R	Requires attention		

4.3 Application of the control framework and model

As discussed in the methodology (Section **Error! Reference source not found.**), Web 2.0 technology was mapped against both CobiT and the Trust Services' criteria and associated control objectives relating to intrusion risks. These objectives were used to identify relevant risks and internal control measures.

In applying the frameworks, consideration was given to the following CobiT objective: '*DS5 - To ensure system security,*' to safeguard against unauthorised use, disclosure or modification, damage or loss and to ensure access is restricted to authorised users (CobiT, 2007). Control over the IT process for ensuring systems security that satisfies the business requirement of safeguarding information against unauthorised use, disclosure or modification and damage or loss is enabled thought logical access controls which ensure that access to systems, data and programs is restricted to authorised users. CobiT is successful at a high level in addressing the security risks posed by unauthorised entry and the disclosure of confidential information. It clearly shows what should be managed thought its control objectives, but does not show how to design, implement and maintain a risk management system.

Trust Services' criteria is used as a model to focus on these areas. To apply Trust Services' criteria to manage intrusion risk, it was necessary to look at the following:

- *Security*: The system is protected against unauthorised logical and physical access.
- *Online privacy*: Personal information obtained as a result of e-commerce is collected, used, stored and disclosed as committed.
- *Confidentiality*: Information designated as confidential is protected as committed (AICPA/CICA, 2003).

Trust Services' criteria provides an adequate framework for how security, online privacy and confidentiality can be achieved; control techniques must still be implemented and will depend on the context of the environment. In a Web-centric environment, control techniques would be mainly automated and could consist of preventative, detective and remedial controls.

These objectives, principles and criteria are not the only objectives that are relevant to intrusion risks. However, the most significant intrusion risks can be identified by focusing on these control objectives above. The results of this process of applying the control framework, control model and related control techniques are summarised in appendix A and are discussed in the following sections.

5. RISKS AND RECOMMENDED SAFEGUARDS

Before discussing the intrusion risks specific to Web 2.0 technology, it is necessary to outline the other risks which internet users are exposed to.

5.1 Risks of the Internet

Web 2.0 exposes businesses to new threats, developed specifically to target Web 2.0 technologies (Clearswift, 2007a). However, the same vulnerabilities that affect traditional web applications also impact on Web 2.0 applications (Hewlett-Packard, 2007; Clearswift, 2007b) and expose a company to the following potential risks and consequences:

- Security threats relating to electronic intrusion by, for example, hackers or malicious software;
- Placing reliance on software that does not reside in a company's domain and its potential impact on the continuity of operations, because few websites offer service-level guarantees; moreover, support is limited;

- The continuously updating user interface may negatively impact on the applications' performance;
- Shortages of technical skills and resources required to ensure that the infrastructure operates effectively, are maintained and upgraded;
- Software and websites may neither be adequately tested; nor may the newest patches be loaded;
- Data leakage and loss of confidentiality and privacy. This could result in brand damage, pose a threat to the company's reputation or a loss of intellectual property;
- Untrustworthy information sources that might contain factual inaccuracies and errors, impacting on the credibility, ethics and legality of web content, while the ability to combine information from various sources could result in a decrease in relevance of content;
- Unproductive use of company assets (i.e. resources) and employee time, including losses arising from a discontinuation of operations;
- Exposing a business to legal liability and financial penalties from regulatory compliance breaches, including copyright breaches or plagiarism (Rudman, 2007b).

5.2 Security and hacker risk

The risks in Section 5.1 represent internal threats, including authorised users performing unauthorised activities, as well as abusing authority. Also listed are external threats. Security breaches involve the stealing or illegally offering data to those who never intended to have it (Bradley, 2008). This study focuses on security risks, specifically on the risks posed by hackers. A hacker is typically defined as someone who attempts to break into a computer system because of his/her proficiency in programming or sufficient technical knowledge to identify weaknesses in a system (Lamprecht, 2004). In essence, a hacker is an unauthorised person intruding into a company's domain and performing unauthorised acts. The focus of web-based attacks has shifted to applications running on the web server and the data systems that support the website by exploiting flaws in website design. This can occur by means of embedding objects into webpages/applications, launching malware *et cetera*.

For several years, the security industry has focused on securing corporate e-mail gateways, firewalls and perimeter protection. At the same time, web application developers give less consideration to security, and rather focus on functionality (Livshits & Erlingsson, 2007). The same characteristics that enable creativity, productivity and collaboration, make Web 2.0 applications prone to attack (Chess, 2008, Pescatore & Feiman, 2008) and provide new delivery platforms and widens the attack surface (Livshits & Erlingsson, 2007). This enables hackers to consider alternative channels to access information (Firstbrook, 2007). The growth in avenues for attacks can be attributed to the availability of potentially dangerous technologies and change in the nature and the manner in which the Internet is used.

Using the framework discussed in section 3, the following risks and related consequences, specific to intrusion risks in Web 2.0 applications, were identified and are presented in table 2.

Table 2. **Web 2.0 risks classified in terms of the feature that gives rise to the risk**

Risks	Consequences
1. XML poisoning or injection, where malicious code is injected during the creation of an application. 2. Dynamic code obfuscation where randomly generated source code is created. 3. Widget exploitations, where widgets with malicious code included, are re-used. 4. RSS-injection, where malicious code is injected into the RSS-feed.	Web 2.0 allows for the easy re-combination of content, source code and applications, which code can be injected into a system.
5. Programming language that is easy to understand, with tools that can be used to debug and analyse source code, is freely available online, which can be used to identify weaknesses. 6. Technical support, blogs *et cetera* explaining coding are available online.	Ability to analyse and obtain an understanding of source code vulnerabilities makes it easy for attackers to identify weaknesses in the source code.
7. Cross Site Scripting with AJAX or XPath which could result in a code injection. 8. AJAX superworms that search IP addresses to identify vulnerabilities and inject a Cross Site Scripting attack. 9. Cross Site Request Forgery where hackers simulate authorised requests. 10. AJAX bridging when a vulnerability in a bridge is exploited to send requests.	Self-initiation of instructions and requests makes it harder for a users' system to identify and authenticate requests and the source of the requests.
11. Unnecessary features create security weaknesses. 12. SSL blindspots where malicious software is not scanned, because the threat is delivered by means of encryption. 13. Weaknesses in the service provider controls are exploited. 14. Poor or incorrect configuration of browser security settings. 15. An increase in the number of devices relying on browser technology, which increases the number of devices and entrance points to secure.	Poor or incorrect set-up of client and server-side controls could result in intruders identifying weaknesses.
16. Socially engineered-led malware using information submitted to Web 2.0 sites to launch attacks.	Availability of personal information could aid in designing socially engineered-led malware.

All users of Web 2.0 applications are exposed to the vulnerabilities, including subsequent users that are exposed to the code. These code injections can include, amongst others, poisoned cookie theft, keystroke logging, Trojan horses, Spam over Instant Messaging (SpIM), screen scraping and denial of service attacks. Once the malicious code is injected onto the user's system, it can process requests, which could fool other websites as originating from legitimate users automatically, reprogram firewalls, routers *et cetera* to permit other outside access.

The risks, relating specifically to Web 2.0 applications, appear to be similar to the risks that existed previously on the Internet, however, due to the unique nature of Web 2.0 technologies, new understanding and control framework is required to protect against the new vulnerabilities.

5.3 Recommended safeguards

In order to mitigate the risks identified in Section 5.1 and 5.2, it is necessary to apply the control framework and model to the technology and thereby identifying control techniques to reduce the risk to an acceptable level. Web 2.0 security impacts every aspect of information technology, ranging from data security to device security (on all end-points such as cellphones, PDAs) to connectivity security (all networks and perimeters) (Davidson & Yoran, 2007).

Web 2.0 applications place a greater reliance on the controls implemented on the client-side and on the security features of the browser than on server-side controls; consequently, a multi-layered approach should be implemented to address the risks at a gateway and at a desktop level, as well as all devices (Cluley, 2007). The threats can be addressed by using technological solutions, but must be complimented by an administrative component and should consist of a combined approach.

Table 3 highlights the controls which need to be implemented to mitigate the Web 2.0 specific risks and affected areas.

Table 3. **Summarised controls and affected areas**

Safeguards	Affected area
1. Implement a robust policy governing the use of Web 2.0 applications.	Policy implementation
2. Educate users on the risks associated with Web 2.0 applications and related safeguards.	User-education
3. Monitor and review resource activity, as well as following up on all logs and audit trails.	Monitor and review
4. Ensure that all network and software (including the latest patches) are frequently updated.	Network security
5. Utilise all browser security features and ensure the browser is correctly configured.	Browser security

6. Utilise all security features that the Web 2.0 application has available and ensure that the application is correctly configured. 7. Implement input validation and other technological driven controls. 8. Sign a service level agreement with service providers of frequently used Web 2.0 applications.	Program security
9. Block access to designated websites, file types and utilities. 10. Implement a next generation reputation based filtering of all forms of incoming and outgoing communications. 11. Utilise deep-scanning heuristic and behavioural anti-malware programs.	Security software
12. Review the source code of frequently used websites and remain involved in the open-source community and search support websites for vulnerabilities. 13. Develop a best practices framework for the utilisation and creation of Web 2.0 applications.	Development and maintenance controls

CONCLUSIONS

The Internet is inherently risky, with a company being able to limit its exposure to some extent. Web 2.0 has entered the corporate mainstream, continually changing and evolving. Its impact is real. Security must evolve with it. The objective of this study is to develop a framework to identify the significant intrusion risks, arising from the use of Web 2.0 technologies and to recommend possible safeguards to mitigate these risks of unauthorised access.

As with any information privacy and security program, there is no one size fits all solution. Every organisation, technology and application is unique and the safeguards depend on the nature of the organisation, information at stake, degree of vulnerability and risks. A proper control environment for managing intrusion risks must consist of a control framework such as CobiT that indicates what should or should not be done; a control model such as Trust Services' criteria to focus on the design, implementation and maintenance controls to manage the risks and control techniques appropriate to address the control objectives. The application of this, results in a comprehensive security program which would include, at a minimum, the following:

1. A multi-layer approach relying on technological safeguards, such as anti-malware programs and a combination of filters that perform deep analyses of all forms of inbound and outbound communication. Reliance should not only be placed on technology focused on Web 2.0 applications, but all security protocols should be considered, including gateway and desktop safeguards.
2. A Web 2.0 policy should be formulated, implemented and compliance with the policy should be monitored. The policy should be easy to understand, implemented and monitored; yet, detailed enough to be enforceable and be used to hold users accountable.

3. Users should be trained on acceptable Web 2.0 practices and security features.

This framework/security program above outlines principles and procedures that could be used as a starting point to mitigate these ‘new’ risks to an acceptable level.

This research investigated the security risks of Web 2.0 applications. Further research could be performed on the privacy risks and related controls.

REFERENCES

AICPA/CICA (2003) *Trust Services Principles and Criteria,* American Institute of Certified Public Accountants, Inc and Canadian Institute of Chartered Accountants, available on-line at http://www.aicpa.org

Bonatti, P. & Samarati, P. (2002) “A uniform framework for regulating access and information release on the web”, *Journal of Computer Security*, vol. 10, no. 3: 241-271

Bradley, A. (2007) “Key issues in the enterprise application of Web 2.0, practices, technologies, products and services, 2007.”, *Gartner.* Research report, 14 June 2007, available on-line at http://www.gartner.com/DisplayDocument?ref=g_search&id=507237&subref=simplesearch

Bradley, A. (2008) “Five major challenges organizations face regarding social software.”, *Gartner.* Research report. 13 February 2008, available on-line at http://www.gartner.com/DisplayDocument?ref=g_search&id=602207&subref=implesearch

Cavoukian, A. & Tapscott, D. (2006) “Privacy and the Enterprise 2.0.”, *New Paradigm Learning Corporation*. White paper. 17 October 2006, available on-line at http://newparadigm.com/media/Privacy_and_ the_Enterprise_2.0.pdf

Chess, B. (2008) “Assessing application vulnerabilities: A 360 degree approach”, *Fortify Software Inc*. White paper, available on-line at http://www.fortify.com/servlet/download/public/Fortify_360 Whitepaper .pdf

Clearswift (2007a) “Content security 2.0: The impact of Web 2.0 on corporate security.”, *Clearswift Limited.* White paper 11 May 2007, available on-line at http://resources.clearswift.com/External Content/Features/Clearswift/9586/200704 SurveyReport_US_1063233.pdf

Clearswift (2007b) “Demystifying Web 2.0.”, *Clearswift Limited.* White paper July 2007, available on-line at http://resources.clearswift.com/ExternalContent/C12CUST/Clearswift/9514/200707 DemystifyingWeb21].0_US_1062190.pdf

Cluley, G. (2007) “New Internet brings security challenges”, *Infosecurity*. March 2007, vol. 4, no. 2: 41

CobiT Steering Committee (2007) “COBIT 4.1. 4.1st edition”, *IT Governance Institute*, available on-line at http://www.isaca.org

Coetzee, M. & Eloff, J. (2005) “An access control framework for web services”, *Information management & computer security,* vol. 13, no. 1: 29-38

Coetzee, M. & Eloff, J. (2007) "Web services access control framework architecture incorporating trust.", *Internet research*, vol. 17, no. 3: 291-305

Committee of Sponsoring Organisations of the Treadway Commission (1992) "Internal control – integrated framework", available on-line at http://www.isaca.org

D'Agostino, D. (2006) "Security in the world of Web 2.0.", *CIO Insight*. Winter. 9 September 2006: 12-15

Davidson, M. & Yoran, E. (2007) "Enterprise security for Web 2.0.", *Computer*. November 2007: 117-119

Dawson, R. (2007) "Web 2.0 framework", available on-line at http://www.rossdawsonblog.com/Web2_Frame work.pdf

Dawson, R. (2008) "An enterprise 2.0 Governance Framework-looking for input!", available on-line at http://rossdawsonblog.com/weblog/archives/2008/02/an_enterprise_2.html

Fanning, E. (2007) "Security for Web 2.0.", *Computerworld*. 3 September 2007: 44

Firstbrook, P. (2007) "The growing web threat", *Gartner*. Research report. 13 April 2007, available on-line at http://www.gartner.com/DisplayDocument?ref=g_search&id=747229&subref=implesearch

Georgia Tech Information Security Centre (2008) "Emerging cyber threat reports for 2008", *Georgia Tech Information Security Centre*. 2 October 2007, available on-line at http://www.gtisc.gatech.edu/ pdf/GTISC%20Cyber%20Threats %20Report.pdf

Ghandi, A. (2008) "Security threats from social computing", *Security*. March 2008: 20-22

Hewlett-Packard (2007) "Securing Web 2.0: are your web applications vulnerable?", *Hewlett-Packard Development Company, L.P.* Whitepaper. October 2007, available on-line at http://www.hp.com/go/ software

Horrigan, J. (2007) "A typology of information and communication users", *PEW/Internet & American life Project*, Princeton Survey Research Association. Research report. 7 May 2007, available on-line at http://www.pewInternet.org/pdfs/PIP_ICT_Typology.pdf

IT Governance Institute (2006) "CobiT mapping: Overview of international IT guidance.", 2nd Edition. *IT Governance Institute*. Illinois, available on-line at http://www.isaca.org

Lamprecht, C. (2004) "Hacker risk in e-commerce systems with specific reference to the disclosure of confidential information.", *South African Journal of Information Management*, vol. 8, no. 4: December 2004

Lee, M. & Lan, Y. (2007) "From Web 2.0 to conversational knowledge management: Towards collaborative intelligence", *Journal of Entrepreneurship Research*. June 2007, vol. 2, no. 2: 47-62

Lenhart, A. & Madden, M. (2007) "Teens, privacy, and online social networks.", Research report. *PEW/ Internet & American life Project.* Princeton Survey Research Association. 18 April 2007, available on-line at http://www.pewInternet.org/pdfs/PIPTeens_Privacy_SNS_Report_Final.pdf

Livshits, B. & Erlingsson, U. (2007) "Using web application construction frameworks to protect against code injection attacks.", *Microsoft research.* Microsoft Corporation. 14 June 2007, available on-line at http://research.microsoft.com/ ~livshits/papers/pdf/plas07.pdf

Matuszak, G. (2007) "Enterprise 2.0: The benefits and challenges of adoption.", *KPMG LLP International.* Whitepaper. 1 May 2007, available on-line at http://us.kpmg.com/microsite/attachments/2008/ Enterprise 20_Adoption.pdf

Metz, C. (2007) "Web 3.0.", *PC Magazine*. 10 April 2007, available on-line at http://www.pcmag.com/ article2/0,2817, 2102852,00.asp

Mitchell, R. (2007) "Web 2.0 users open a box of security risks", *Computerworld*. 26 March 2007: 32

Pescatore, J. & Feiman, J. (2008) "Security features should be built into Web 2.0 applications", *Gartner,* Research report. 5 March 2008, available on-line at http://www.gartner.com/DisplayDocument?ref=g_ search&id=617320&subref= simplesearch

Radcliff, D. (2007) "Are you watching?", *SC Magazine*, September 2007: 40-43

Ratnasigam, P. (2007) "A risk-control framework for e-marketplace participation: the findings of seven cases", *Information management & computer security*, vol. 15, no. 2: 149-166

Rudman, R. (2007a) "Web 2.0: The Internet is versioning.. 1.0, 2.0.", *Accountancy SA*, September 2007: 25-27

Rudman, R. (2007b) "Web 2.0 + Risk = Risk 2.0: Are you protected?", *Accountancy SA*, October 2007: 26-29

Shin, D. (2008) "Understanding purchasing behaviour in a virtual economy: Consumer behaviour involving currency in Web 2.0 communities", *Interacting with computers*, 11 April 2008, vol. 20: 433-446

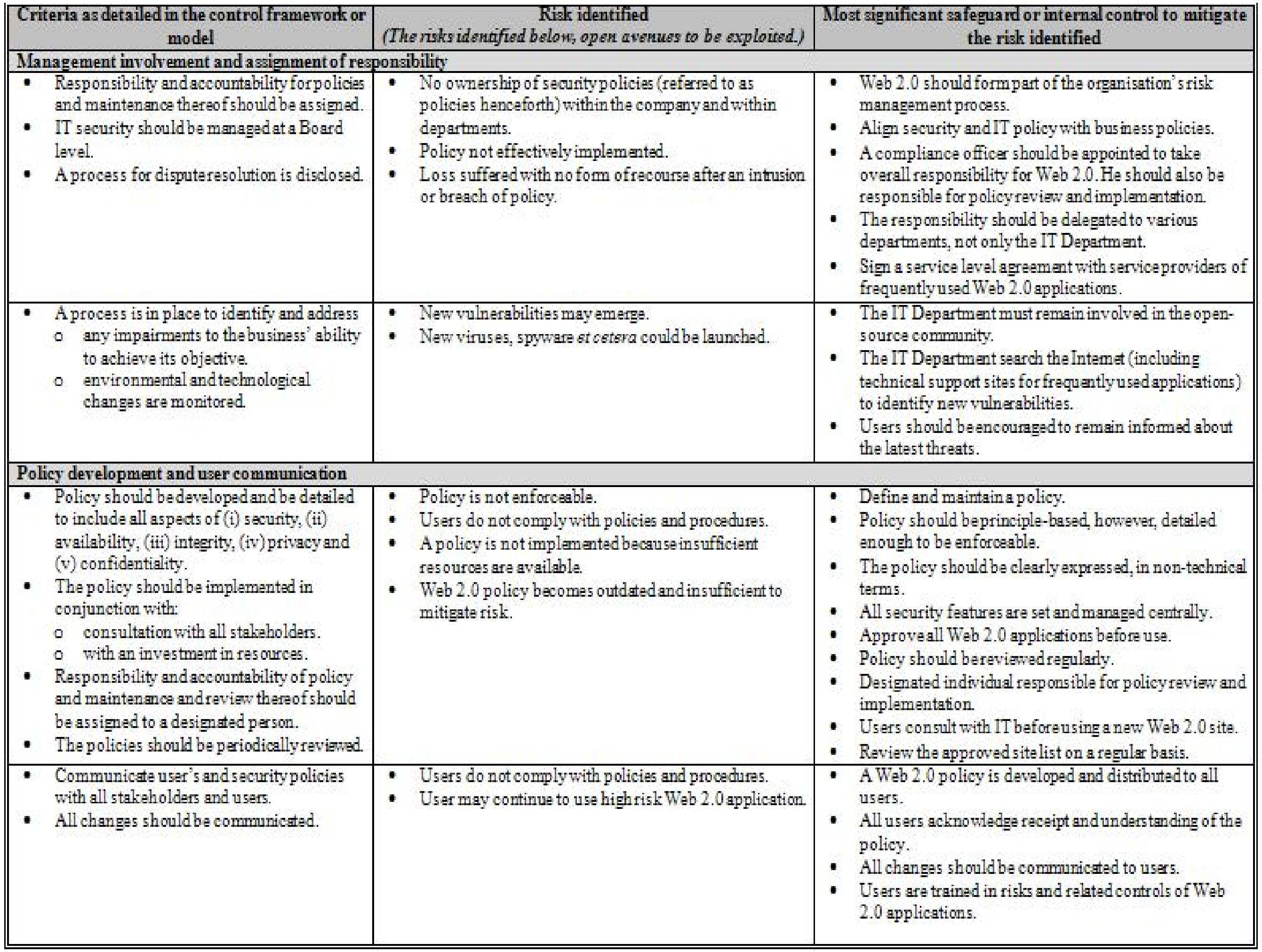
Smith, D. (2008) "Web 2.0 and beyond: Evolving the discussion.", *Gartner.* Research report. 24 January 2008, available on-line at http://www.gartner.com/ DisplayDocument?ref=gsearch&id=588707&subref= simple search

Valdes, R. (2008) "Key issues in rich Internet application platforms and user experience", 2008. *Gartner.* Research report. 25 January 2008, available on-line at http://www.gartner.com/DisplayDocument?ref= gsearch&id=589413 &subref=simplesearch

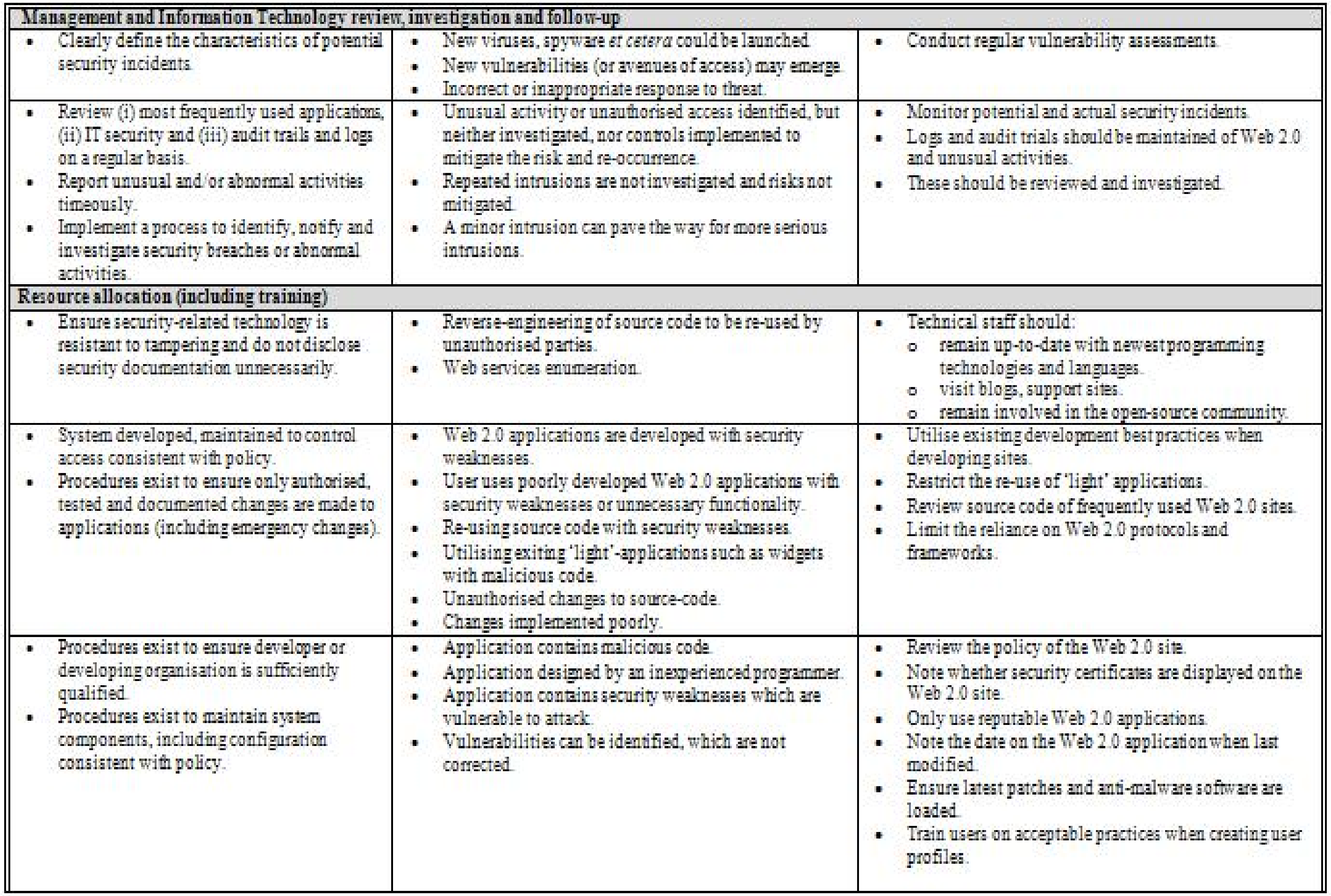
Wikipedia (2008) "Web 2.0.", *Wikipedia*, available on-line at http://en.wikipedia.org/ wiki/Web_2

Appendix A.
Control framework to Web 2.0 applications

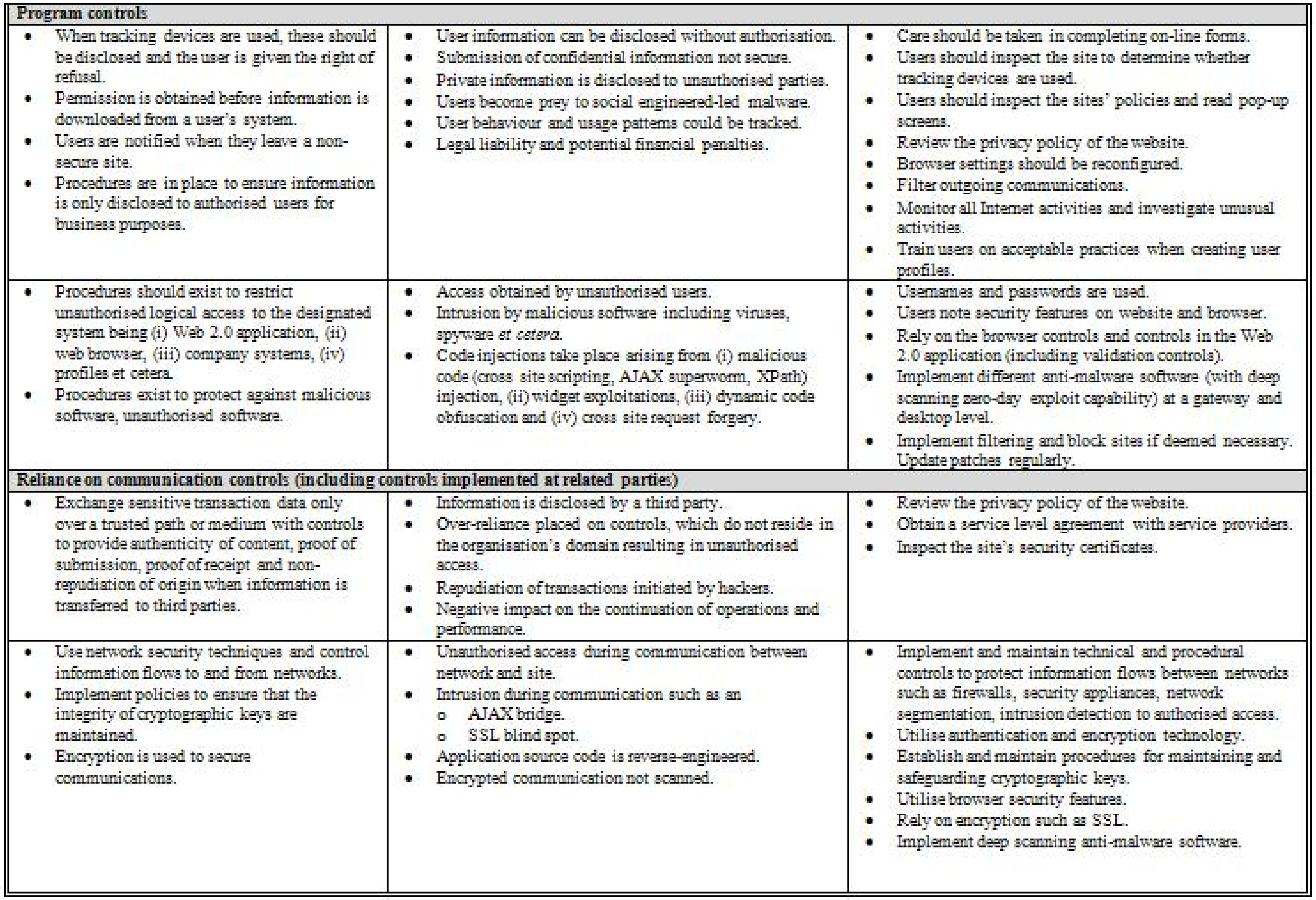
The following table details the risks identified by the application of CobiT and Trust services' to Web 2.0 technology from the perspective of Web 2.0 users and where content is contributed. The tables below are summarised in general terms in order to provide flexibility in applying the principles to specific situations. The tables were specifically constructed with Web 2.0 and the risk with the implication of unauthorised access in mind.



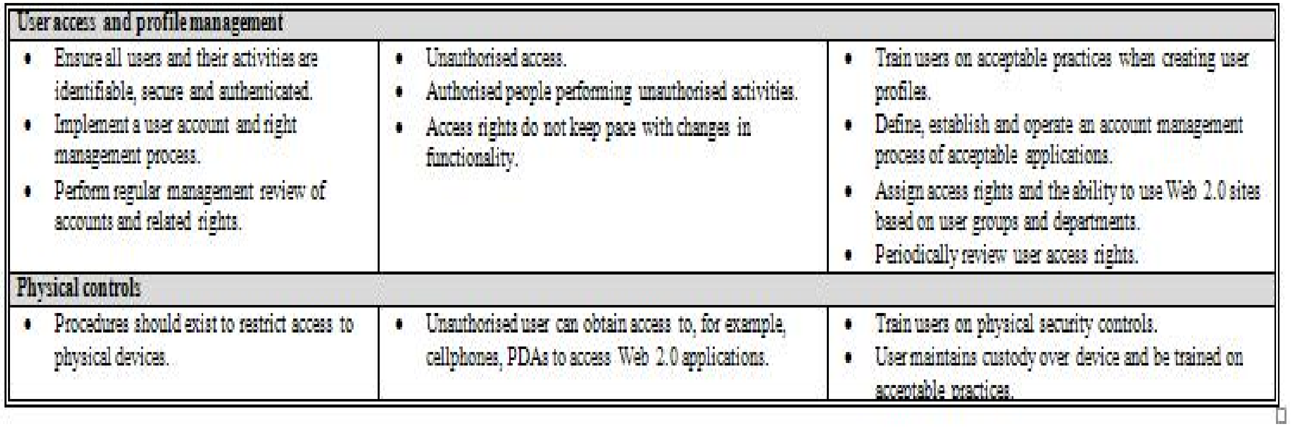
Criteria as detailed in the control framework or model	Risk identified *(The risks identified below, open avenues to be exploited.)*	Most significant safeguard or internal control to mitigate the risk identified
Management involvement and assignment of responsibility		
• Responsibility and accountability for policies and maintenance thereof should be assigned. • IT security should be managed at a Board level. • A process for dispute resolution is disclosed.	• No ownership of security policies (referred to as policies henceforth) within the company and within departments. • Policy not effectively implemented. • Loss suffered with no form of recourse after an intrusion or breach of policy.	• Web 2.0 should form part of the organisation's risk management process. • Align security and IT policy with business policies. • A compliance officer should be appointed to take overall responsibility for Web 2.0. He should also be responsible for policy review and implementation. • The responsibility should be delegated to various departments, not only the IT Department. • Sign a service level agreement with service providers of frequently used Web 2.0 applications.
• A process is in place to identify and address o any impairments to the business' ability to achieve its objective. o environmental and technological changes are monitored.	• New vulnerabilities may emerge. • New viruses, spyware *et cetera* could be launched.	• The IT Department must remain involved in the open-source community. • The IT Department search the Internet (including technical support sites for frequently used applications) to identify new vulnerabilities. • Users should be encouraged to remain informed about the latest threats.
Policy development and user communication		
• Policy should be developed and be detailed to include all aspects of (i) security, (ii) availability, (iii) integrity, (iv) privacy and (v) confidentiality. • The policy should be implemented in conjunction with: o consultation with all stakeholders. o with an investment in resources. • Responsibility and accountability of policy and maintenance and review thereof should be assigned to a designated person. • The policies should be periodically reviewed.	• Policy is not enforceable. • Users do not comply with policies and procedures. • A policy is not implemented because insufficient resources are available. • Web 2.0 policy becomes outdated and insufficient to mitigate risk.	• Define and maintain a policy. • Policy should be principle-based, however, detailed enough to be enforceable. • The policy should be clearly expressed, in non-technical terms. • All security features are set and managed centrally. • Approve all Web 2.0 applications before use. • Policy should be reviewed regularly. • Designated individual responsible for policy review and implementation. • Users consult with IT before using a new Web 2.0 site. • Review the approved site list on a regular basis.
• Communicate user's and security policies with all stakeholders and users. • All changes should be communicated.	• Users do not comply with policies and procedures. • User may continue to use high risk Web 2.0 application.	• A Web 2.0 policy is developed and distributed to all users. • All users acknowledge receipt and understanding of the policy. • All changes should be communicated to users. • Users are trained in risks and related controls of Web 2.0 applications.



Management and Information Technology review, investigation and follow-up		
• Clearly define the characteristics of potential security incidents.	• New viruses, spyware *et cetera* could be launched. • New vulnerabilities (or avenues of access) may emerge. • Incorrect or inappropriate response to threat.	• Conduct regular vulnerability assessments.
• Review (i) most frequently used applications, (ii) IT security and (iii) audit trails and logs on a regular basis. • Report unusual and/or abnormal activities timeously. • Implement a process to identify, notify and investigate security breaches or abnormal activities.	• Unusual activity or unauthorised access identified, but neither investigated, nor controls implemented to mitigate the risk and re-occurrence. • Repeated intrusions are not investigated and risks not mitigated. • A minor intrusion can pave the way for more serious intrusions.	• Monitor potential and actual security incidents. • Logs and audit trials should be maintained of Web 2.0 and unusual activities. • These should be reviewed and investigated.
Resource allocation (including training)		
• Ensure security-related technology is resistant to tampering and do not disclose security documentation unnecessarily.	• Reverse-engineering of source code to be re-used by unauthorised parties. • Web services enumeration.	• Technical staff should: o remain up-to-date with newest programming technologies and languages. o visit blogs, support sites. o remain involved in the open-source community.
• System developed, maintained to control access consistent with policy. • Procedures exist to ensure only authorised, tested and documented changes are made to applications (including emergency changes).	• Web 2.0 applications are developed with security weaknesses. • User uses poorly developed Web 2.0 applications with security weaknesses or unnecessary functionality. • Re-using source code with security weaknesses. • Utilising exiting 'light'-applications such as widgets with malicious code. • Unauthorised changes to source-code. • Changes implemented poorly.	• Utilise existing development best practices when developing sites. • Restrict the re-use of 'light' applications. • Review source code of frequently used Web 2.0 sites. • Limit the reliance on Web 2.0 protocols and frameworks.
• Procedures exist to ensure developer or developing organisation is sufficiently qualified. • Procedures exist to maintain system components, including configuration consistent with policy.	• Application contains malicious code. • Application designed by an inexperienced programmer. • Application contains security weaknesses which are vulnerable to attack. • Vulnerabilities can be identified, which are not corrected.	• Review the policy of the Web 2.0 site. • Note whether security certificates are displayed on the Web 2.0 site. • Only use reputable Web 2.0 applications. • Note the date on the Web 2.0 application when last modified. • Ensure latest patches and anti-malware software are loaded. • Train users on acceptable practices when creating user profiles.



Program controls		
• When tracking devices are used, these should be disclosed and the user is given the right of refusal. • Permission is obtained before information is downloaded from a user's system. • Users are notified when they leave a non-secure site. • Procedures are in place to ensure information is only disclosed to authorised users for business purposes.	• User information can be disclosed without authorisation. • Submission of confidential information not secure. • Private information is disclosed to unauthorised parties. • Users become prey to social engineered-led malware. • User behaviour and usage patterns could be tracked. • Legal liability and potential financial penalties.	• Care should be taken in completing on-line forms. • Users should inspect the site to determine whether tracking devices are used. • Users should inspect the sites' policies and read pop-up screens. • Review the privacy policy of the website. • Browser settings should be reconfigured. • Filter outgoing communications. • Monitor all Internet activities and investigate unusual activities. • Train users on acceptable practices when creating user profiles.
• Procedures should exist to restrict unauthorised logical access to the designated system being (i) Web 2.0 application, (ii) web browser, (iii) company systems, (iv) profiles et cetera. • Procedures exist to protect against malicious software, unauthorised software.	• Access obtained by unauthorised users. • Intrusion by malicious software including viruses, spyware *et cetera.* • Code injections take place arising from (i) malicious code (cross site scripting, AJAX superworm, XPath) injection, (ii) widget exploitations, (iii) dynamic code obfuscation and (iv) cross site request forgery.	• Usernames and passwords are used. • Users note security features on website and browser. • Rely on the browser controls and controls in the Web 2.0 application (including validation controls). • Implement different anti-malware software (with deep scanning zero-day exploit capability) at a gateway and desktop level. • Implement filtering and block sites if deemed necessary. Update patches regularly.
Reliance on communication controls (including controls implemented at related parties)		
• Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin when information is transferred to third parties.	• Information is disclosed by a third party. • Over-reliance placed on controls, which do not reside in the organisation's domain resulting in unauthorised access. • Repudiation of transactions initiated by hackers. • Negative impact on the continuation of operations and performance.	• Review the privacy policy of the website. • Obtain a service level agreement with service providers. • Inspect the site's security certificates.
• Use network security techniques and control information flows to and from networks. • Implement policies to ensure that the integrity of cryptographic keys are maintained. • Encryption is used to secure communications.	• Unauthorised access during communication between network and site. • Intrusion during communication such as an o AJAX bridge. o SSL blind spot. • Application source code is reverse-engineered. • Encrypted communication not scanned.	• Implement and maintain technical and procedural controls to protect information flows between networks such as firewalls, security appliances, network segmentation, intrusion detection to authorised access. • Utilise authentication and encryption technology. • Establish and maintain procedures for maintaining and safeguarding cryptographic keys. • Utilise browser security features. • Rely on encryption such as SSL. • Implement deep scanning anti-malware software.



User access and profile management		
• Ensure all users and their activities are identifiable, secure and authenticated. • Implement a user account and right management process. • Perform regular management review of accounts and related rights.	• Unauthorised access. • Authorised people performing unauthorised activities. • Access rights do not keep pace with changes in functionality.	• Train users on acceptable practices when creating user profiles. • Define, establish and operate an account management process of acceptable applications. • Assign access rights and the ability to use Web 2.0 sites based on user groups and departments. • Periodically review user access rights.
Physical controls		
• Procedures should exist to restrict access to physical devices.	• Unauthorised user can obtain access to, for example, cellphones, PDAs to access Web 2.0 applications.	• Train users on physical security controls. • User maintains custody over device and be trained on acceptable practices.