UNIVERSITY OF WATERLOO

Technology Risk Assessment Methodologies

ACC626, Term Paper

Diana Hanna

7/3/2013

Contents

Technology Risk Assessment Methodology

Technology is forever changing, or so it seems. Due to the rapid pace in which this growth is occurring, companies who want to keep up to date must also deal with the risks of new and potentially untested technology[1]. As many companies will have experienced through their lifetime, IT investment costs are high; generally systems are expensive to implement and maintain, and the ROI is difficult to estimate. The challenge lies in the entity's ability to assess the risks they are exposed to with the system, and their ability to manage those risks to increase the value added of their IT systems.

IT risk affects all levels of the organization, but can be strongly linked to business processes and strategy[2]. A focus has been put on IT governance due to its pervasive qualities, and the ability of an IT failure to affect the business processes of the entire organization[3]. There are many examples of situations where an IT failure has caused financial damage to corporations, such as a drop of $2.5 billion in market value when E*Trade experienced a power outage[4]. Thus, IT risk is a topic of interest for upper management and c-suite executives, and should be considered when implementing a company-wide risk assessment and management framework.

There are many risk assessment frameworks available, but few stand out as "formal IT risk-assessment frameworks" as identified by CSO Online[5] and ISACA. These include OCTAVE, FAIR, RMF, TARA[6] and Risk IT and will be discussed later on in further detail. Another topic of discussion will be the ability of organizations to effectively integrate their IT risk assessments into overall company risk models, such as COSO[7], COBIT, and the All Hazards Risk Assessment (AHRA).

Assessment and management of risks associated with technology

The initial assessment of IT risk is imperative in understanding how the company should move forward with management. First, it is important to define IT risk, so that a benchmark is defined when discussing the frameworks. ISACA defines IT risk as the "business risk related to the use of IT"[8]. Considering the growth of information technology, and how it has become so pervasive, the impact of IT can be seen in all aspects of an organization, including financial, reputational, regulatory, customer, and competition; despite the impacts, IT is critical to organizational development[9]. To fully assess impact of risks, as well

[1] Boritz, Jefim Efrim. 5.5.
[2] ISACA. "ISACA: Serving IT Governance Professionals." ISACA Issues COBIT 5 Governance Framework.
[3] Trautman, Lawrence James. p4.
[4] Boritz, Jefim Efrim. 2.12.
[5] Violino, Bob.
[6] Violino, Bob.
[7] Curtis, Dr. Patchin, Mark Carey, and Deloitte &Touche LLP.
[8] ISACA. "ISACA: Serving IT Governance Professionals." Risk Assessment.
[9] Jordan, Ernest. p3.

as their willingness to take them on, companies would benefit from a risk assessment and management frameworks.

A general framework for practical risk assessment is the Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM Risk Assessment in Practice. COSO is the most widely known risk framework. Despite its enterprise-wide focus, it does provide a general approach to risk assessment that can be used in many functional risk assessments. The CICA's IT General Controls (ITGC) as discussed by Dr. J.E. Boritz[10] will be used to shed further light on the IT-specific risks associated with a company.

Risk Assessment

A general approach to risk assessment has been identified by COSO for ERM Risk Assessments using a Process flow diagram, as seen in **Figure 1**[11].

Figure 1

Identifying risks is the initial step. As noted, IT risks are pervasive, and so may need to be identified in individual departments of the organization, rather than just the IT department (i.e. authorization process in A/R, use of spreadsheets in purchasing, etc.). This is made evident in all mediums (textbooks, papers, articles, journals, etc.), most notably:

> *"IT is increasingly becoming a factor that contributes to business process effectiveness, not just a means for achieving processing efficiency."*[12]

As this is the case, it is now critical to test and ensure IT is performing at its highest potential to provide an entity with a competitive advantage, or at the least to keep with industry standards. To do so, Boritz also notes that metrics need to be identified to ensure that IT is performing as well, or better than, industry averages; if not, then mitigant strategies need to be taken to better the technology. An "IT Balanced Scorecard", as shown in **Figure 2**[13], is an example of how to lay out performance metrics for the purposes of information technology benchmarking.

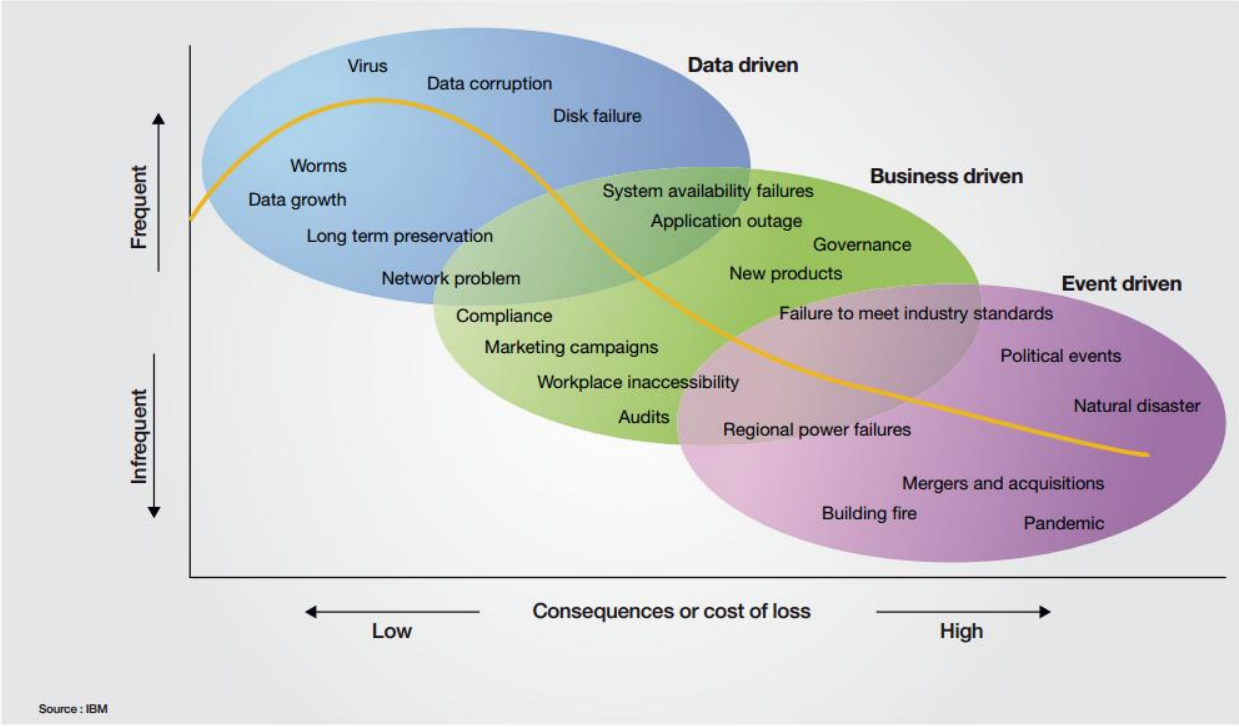
[10] J. Efrim Boritz, BA, MBA, PhD, FCA, CA•CISA, CA•IT
[11] Curtis, Dr. Patchin, Mark Carey, and Deloitte &Touche LLP. p2.
[12] Boritz, Jefim Efrim. 6.9. Print.
[13] Boritz, Jefim Efrim. 6.10. Print.

Figure 2 – IT Balanced Score Card Example

IT Balanced Scorecard			
Financial Metrics	Customer Metrics	Process Metrics	Learning Metrics
• # of IT customers	• Level of service delivery up	• Availability of systems & services	• Staff productivity & morale
• Cost per IT customer	• Satisfaction of existing customers	• Developments on schedule & budget	• # of staff trained in new services
• Cost-efficiency of IT processes up	• # of new customers reached	• Throughput & response times	• Value delivery per employee up
• Delivery of IT value per employee channels	• # of new service delivery channels	• Amount of errors and rework	• Increased availability of knowledge systems

Specific to IT, there are 3 types of threats: Data-driven risks (system/data level), business-driven risks (business operations/continuity) and event-driven risks[14]. Frequency and consequences of loss from each type (as well as examples of each) are identified in **Figure 3**[15]. This risk identification will assist in the creation of a risk hierarchy (discussed below) by risk type.

Figure 3 – Graph of Different Types of Risk



[14] IBM. p3.
[15] IBM. p4.

Identification is then followed by the first step in risk assessment; developing assessment criteria. This step is required to prioritize key risks for senior management and board members[16].

There is importance placed on risk being a function of likelihood and impact, yet this function is also criticised for not being the big picture; that there are other factors involved in assessing risk[17]. COSO provides that developing an assessment scale is necessary to create a standard of comparison; items including impact, likelihood, vulnerability, speed of onset (velocity), and inherent and residual[18] are shown as assessment criteria. These criteria assist in creating mitigating factors if any of the results fall below standards.

Next, the company must assess the risk. As this differs per organization, this section will be subjective to each individual assessment. For example, industry average may be 15 months for the implementation of an ERP, but due to the size, effort, and unforeseen circumstances, the company can use a range (i.e. 10-20 months) to maintain realistic benchmarks. This will help the company in identifying whether they fall within or outside of a standard.

Benchmarking is critical to identifying where the IT standards of a company fall within industry. As Boritz notes, a company may be content with their current IT performance, but another company "may have found a better way to do things"[19]. The identification process will bring out the gaps, and the next process, assessment, will confirm the validity of the risk (i.e. is it something to mitigate?). Other qualitative and quantitative criteria include analysis of existing data, surveys, interviews/workshops, scenario analysis, and causal at-risk models[20].

An assessment of the impact following the assessment of risks needs to be completed. As previously discussed, IT is pervasive, and considering an enterprise-wide approach to IT risk assessment would benefit the company in realizing the impacts of all IT risks. COSO recommends the use of risk interaction maps[21] or a big picture analysis (i.e. Fault trees, event trees, bow-tie diagrams)[22]. The understanding of the risk integration will assist management in preparing the best form of risk management to prevent, detect and correct[23].

[16] Curtis, Dr. Patchin, Mark Carey, and Deloitte &Touche LLP. p2.
[17] Curtis, Dr. Patchin, Mark Carey, and Deloitte &Touche LLP. p3.
[18] Curtis, Dr. Patchin, Mark Carey, and Deloitte &Touche LLP. p3-7.
[19] Boritz, Jefim Efrim. 6.10. Print.
[20] Curtis, Dr. Patchin, Mark Carey, and Deloitte &Touche LLP. p9-11.
[21] Curtis, Dr. Patchin, Mark Carey, and Deloitte &Touche LLP. p12.
[22] Curtis, Dr. Patchin, Mark Carey, and Deloitte &Touche LLP. p13.
[23] Appendix I, Question 5

To prioritize risks, again, COSO suggests the use of risk hierarchies; where risk might often be organized within an organizational unit, risk type, geography or strategic objective[24]. An example of risk hierarchies is provided in Appendix II[25]. Another form of prioritization takes the form of a "Risk and Opportunity Map", identifying both Impact (opportunities and risks) and Likelihood; Appendix III provides an example[26] . Other examples are provided within the COSO document, and should be referenced for further examples (i.e. heat maps, MARCI chart).

Risk Management

The next step is to ensure we can manage the prioritized risks. A suggested approach is to bring "together all of the IT risks into a single portfolio [to reduce] the chance of some area of risk being overlooked"[27], suggesting that a high level overview of IT risk will assist in illustrating how much IT risk is actually integrated into the business, and so will increase emphasis on IT risk management within the company[28].

"A successful IT risk mitigation program consists of five phases: Management and governance, assessment, planning and design, implementation and testing, and monitoring... IT risk management and governance is the process by which an appropriate IT risk posture is maintained long term". Management and governance include strategies to ensure all levels of operations are on board with the risk mitigation strategies, both explicitly (in policies) or implicitly (within processes). Assessment encapsulates the discussion above. Planning and design consider the sustainability of IT and how to structure future investments in IT to balance with the business value. Implementation and testing allow the company to put the management design into practice, and identifying weaknesses. Monitoring ensures detection of any risks and continued preventative and corrective actions[29].

It is important to mention that there are multiple methods of risk management, four major categories being acceptance, mitigation, transference, and avoidance[30]. Mitigation is the reduction of risk internally, as discussed above. First, acceptance is the company retaining the risk and budgeting around it, for example providing a reserve for anything that might happen (i.e. flooding, power outages, etc.). Transference is the sharing of IT risk with other parties by outsourcing activities such as security, webtrust/systrust services, IT project management, even risk assessments. Avoidance is the ability of the company to completely eliminate their exposure to risk by removing themselves from the activity; i.e.

[24] Curtis, Dr. Patchin, Mark Carey, and Deloitte &Touche LLP. p14.
[25] Curtis, Dr. Patchin, Mark Carey, and Deloitte &Touche LLP. p14.
[26] Curtis, Dr. Patchin, Mark Carey, and Deloitte &Touche LLP. p15.
[27] Jordan, Ernest. p5.
[28] Jordan, Ernest. p5.
[29] IBM. p5.
[30] Spivey, Jeff.

pushing implementation projects, or not entering a certain industry that may require a higher level of IT knowledge. Where avoidance might be an issue is in the case where the company may lose an opportunity to gain a competitive advantage by penetrating a new market, or having more efficient operations.

Something to note, is a company's risk appetite. This will dictate how much of the risk the company is willing to take on, where and how they prioritize risks, and should come from the objectives of the company and its stakeholders[31]. It is expected that risks are inherent in any company, especially a growing one, and IT is critical in ensuring that a company doesn't suffer growing pains. A successful IT management strategy will minimize risk and optimize opportunities.

Risk assessment models and methodologies

Several formal risk assessments stand out in IT risk assessment, as will be discussed below, that allow companies to identify, assess and manage risk in an IT environment. The following are considered under the "mitigation" strategy method, and are performed internally (or with the help of consultants).

Methodologies

OCTAVE - Operationally Critical Threat, Asset and Vulnerability Evaluation

"The confidentiality, integrity and availability of information are critical to organizations' missions"[32]. OCTAVE "is a risk-based strategic assessment and planning technique for information security. It is self-directed, meaning that people from within the organisation assume responsibility for setting the organisation's security strategy"[33]. The original OCTAVE method has 3 phases, including the organizational view, leading into the technological view, leading into risk analysis; generally created for the "multi-layered hierarchy" company that maintains "their own computing infrastructure"[34]. The three (3) phases include eight (8) processes designed to bring together operations staff and IT professionals to focus on "strategic, practice-related issues"[35].

The alternative OCTAVE methods include OCTAVE-S, which is geared towards smaller companies with a "flat hierarchy"; this method is based on the original, but only has four (4) processes[36]. The other, OCTAVE ALLEGRO, is like the original with eight processes, but has four (4) phases; establishing drivers, profiling assets, identifying threats, identifying/mitigating the resulting risks[37]. The difference with

[31] Rittenberg, Dr. Larry, Frank Martens. p1.
[32] Panda, Parthajit. p1.
[33] Panda, Parthajit. p3.
[34] Panda, Parthajit. p3.
[35] Panda, Parthajit. p3.
[36] Panda, Parthajit. p4.
[37] Panda, Parthajit. p4, figure 5.

ALLEGRO is the information-centricity and the use of "information containers"[38]. This method is meant "improve an organization's ability to perform risk assessment in a more efficient and effective manner" and improve ease of use[39] . Appendix IV shows the original approach, as well as the ALLEGRO approach to OCTAVE.

Noted is the downside to OCTAVE as being complex to implement, and does not allow organizations to model risk mathematically; it is a "qualitative methodology"[40].

FAIR – Factor Analysis of Information Risk

FAIR is a "framework for understanding, analysing and measuring information risk"41. The main idea behind FAIR is consistency; for example, it applies a taxonomy for threats, vulnerabilities and risks so that all individuals involved in the risk assessment "speak the same language". It is meant to

> *"apply risk assessment to any object or asset; view organizational risk in total; defend or challenge risk determination using advanced analysis; and understand how time and money will affect the organization's security profile"*[42]

The goal is have be business-focused, and the consistency of the framework allows all individuals to see the risk exposures in the same light. FAIR also steers clear of ordinal scales, and instead uses "dollar estimates for losses and probability values for threats and vulnerabilities"[43]. This allows for a mathematical analysis of risks, where OCTAVE does not.

On the other hand, FAIR is said to be difficult to use and lacks documentation, something OCTAVE is well known for. Also, FAIR seems to have very little accessible information regarding application and methodology, and so is difficult to implement and maintain.

NIST RMF – National Institute of Standards and Technology's Risk Management Framework

The NIST RMF is an assessment and management methodology that is a series of activities. The activities are "related to managing organizational risk"[44]. NIST notes that they "can be applied to both new and legacy information systems"[45]. These activities are identified in **Figure 4**; to summarize, it requires

[38] Panda, Parthajit. p4.
[39] Panda, Parthajit. p4.
[40] Violino, Bob.
[41] Violino, Bob.
[42] Violino, Bob.
[43] Violino, Bob.
[44] Violino, Bob.
[45] Violino, Bob.

categorizing ISs, selecting, implementing and assessing controls, authorizing IS operations, and then monitoring and assessing specific controls[46].

Figure 4 – NIST RMF Activities

Categorizing	information systems and the information within those systems based on impact.
Selecting	an initial set of security controls for the systems based on the Federal Information Processing Standards (FIPS)
Implementing	security controls in the systems.
Assessing	the security controls using appropriate methods and procedures
Authorizing	information systems operation based on a determination of the risk to organizational operations and assets
Monitoring/ Assessing	selected security controls in information systems on a continuous basis

"NIST is the federal technology agency that works with industry to develop and apply technology, measurements, and standards."[47] As such, the framework created by this agency is considered invaluable, and is one of the positives of the RMF. "The framework is constantly being reviewed and updated as new technology is developed and new laws are passed" because the agency that has created is focusing on cost-effectiveness and high adaptability; and with the stability of application, "software development companies are more willing to develop...tools to support the framework"[48].

Another positive of the framework is it helps to identify where the highest risk lies in the case of security breach. Unfortunately, the RMF is a document, it is not automated, and so the risk analysis is dependent on the users to ensure it is being used consistently and maintenance of risks is being done frequently.

TARA– Threat Agent Risk Assessment

TARA is focused on the only the most likely exposures, as mitigating all risks is thought to be too expensive and impractical. This is a newer framework, created by Intel, that "[distills] the immense number of possible information security attacks into a digest of only those exposures that are most likely to occur"[49]. This is similar to an external audit, in that samples are taken from the most risky areas, and then tested.

[46] Violino, Bob.
[47] www.nist.gov
[48] Violino, Bob
[49] Violino, Bob

Where TARA differs is its ability to identify where the most exposure lies, by first attempting to identify threats, their goals and methods used. Management is then encouraged to focus on these areas, effectively increasing the effect of security strategy, while minimizing efforts[50]. The 3 main benefits of TARA are its abilities to "[distill] the cloud of potential attacks, improve quality of risk and control evaluations, and [better communicate] risks and recommendations to management"[51]. TARA is not meant to replace other methodologies, it is actually meant to complement current organization tools for risk assessment[52]. The "awareness of the most exposed areas" allows a company to create strategies for better decision making regarding risk and risk management, including areas such as budgeting and resource allocation.

To be predictive, TARA has three reference libraries. The "threat agent library...defines eight common threat agent attributes and identifies 22 threat agent archetypes"[53]. The common exposure library identifies many known exposures and vulnerabilities previously identified at Intel. Finally the "methods and objectives library" is used for "known objectives of threat agents and the methods they are most likely to use to accomplish these goals"[54]. Reviews for TARA are generally positive, noting TARA's ability to be integrated into other frameworks in an organization, its ease of use, and the libraries are noted as incredibly useful to also provide standardization on "common threat agents and corresponding methods"[55].

Despite the positive reviews, some drawbacks include TARA's "focus on threats rather than assets"[56], potentially missing the true risks in an infrastructure, and that it is a newer framework, and so may be untested. It is noted that TARA is yet to be common, and is another qualitative methodology, of which many exist[57].

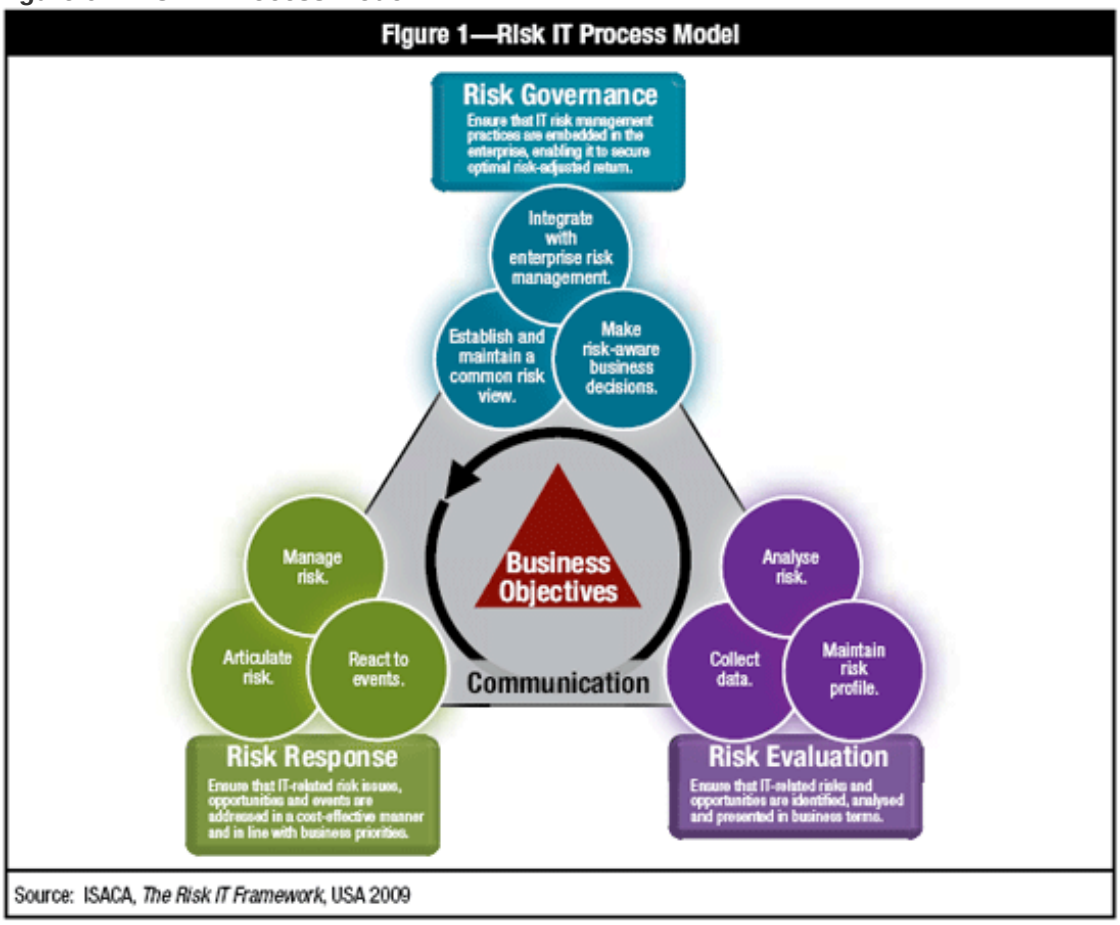
RISK IT

Risk IT is ISACA's initiative to "helping enterprises manage IT-related risk"[58]. It is an initiative that is meant to complement and be integrated with COBIT. COBIT, being the overall "business-driven solution" for IT risks, RISK IT is meant to provide the framework in which to "identify, govern and manage IT Risk"[59]. The RISK IT model is covered very briefly in the excerpt that was provided, but the overarching

[50] Violino, Bob.
[51] Intel.
[52] Intel.
[53] Violino, Bob.
[54] Violino, Bob.
[55] Violino, Bob.
[56] Violino, Bob.
[57] Violino, Bob.
[58] ISACA. The Risk IT Framework Excerpt. p1.
[59] ISACA. The Risk IT Framework Excerpt. p1.

idea is to coordinate risk governance, risk response and risk evaluation. This is noted in **Figure 6**, taken from the RISK IT framework.

Figure 6 – Risk IT Process Model



Company-wide risk models tailored to assess technology risks

COSO ICIF- Committee of Sponsoring Organizations of the Treadway Commission, Internal Control Integrated Framework

ICIF is one of the largest frameworks currently used "to design and assess internal controls"60. Recently the ICIF has gone through a change, to evolve into something from a basic foundation that was laid in the 1992 framework. There are 3 categories of objectives, listed as operations, reporting and compliance objectives[61]. The difference with COSO is that is generally used by SEC compliant organizations to ensure their internal controls are effective. There are five components within the COSO framework, as newly defined in 2013; including control environment, risk assessment, control activities, information and communication, and monitoring activities, which together form the COSO cube, as seen in **Figure 7**.

[60] COSO. p1.
[61] KPMG. p2.

Figure 7 – The COSO Cube

The five components are to work together to create a comprehensive and efficient system of internal controls. IT is fully integrated in the system of internal controls, and is identified under each component when assessing risks. Depending on the organization, each business unit has its own IT risks to assess, and so this is built into the COSO framework to provide an integrated approach towards all risks.

COBIT - Control Objectives for Information and Related Technology

COBIT was created to improve IT efficiency and effectiveness and to align IT with the business. COBIT is a leading industry standard, and is generally used to assess IT risks in many consulting firms; if it is not used, the methodology that is used is generally based on COBIT's ideologies[62].

COBIT 5 – the most up to date version of COBIT – has 5 overarching principles; meeting stakeholder needs, covering enterprise end-to-end, applying a single integrated framework, enabling a holistic approach, and separating governance from management. These are meant to generic principals, to be used and adapted into all sizes of organizations, in all sectors (i.e. for-profit, not-for-profit, public) [63]. The fifth principle provides that governance evaluates needs, directs decision making, and monitors performance (EDM) and management "plans, builds, runs and monitors activities... (PBRM)"[64]. All in all, it is meant to optimise the investment in information technology.

COBIT5 has a family of products that are meant to be used cohesively. For the less capable enterprises, this may be highly costly, and will potentially be too complex; one of the drawbacks of using such a widely known and highly comprehensive framework.

[62] Appendix I
[63] ISACA. "COBIT5 Introduction."
[64] ISACA. "COBIT5 Introduction."

AHRA - All Hazards Risk Assessment (Canada)

In discussing the public sector, specifically federal government institutions, it is a requirement to "conduct mandate-specific risk assessments as the basis for emergency management (EM) planning"[65]. AHRA objectives revolve around risks of federal interest, and so some objectives include:

> *"Enable federal institutions to perform AHRA consistently and efficiently as part of their risk management responsibilities...Capture risks that are significant and are of federal interest...help to foster an AHRA community of practice for the federal community"*[66]

The process is can is linked to the processes identified in ISO 31000 - 'Risk Management – Principles and Guidelines', with the following guidelines:

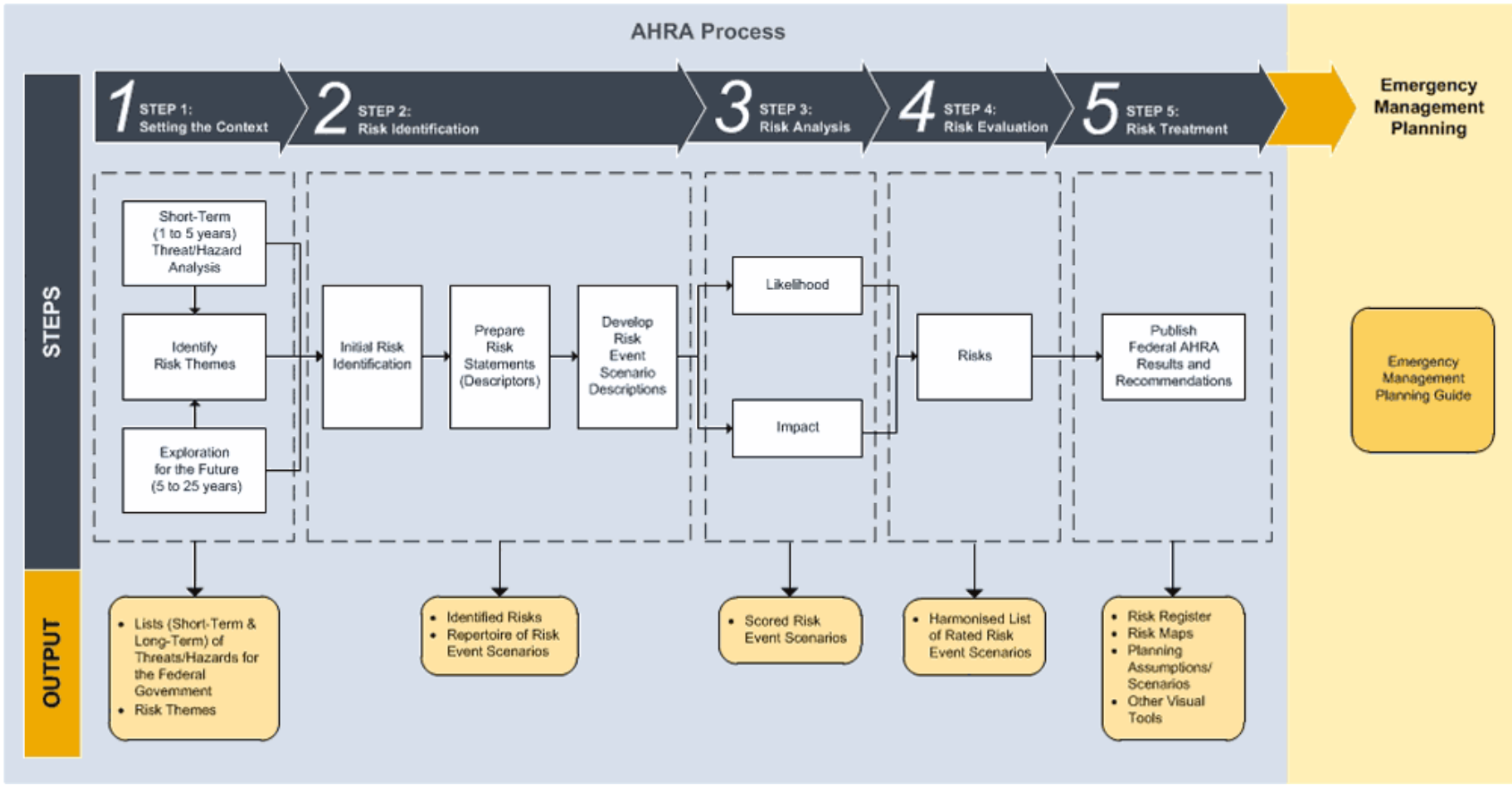
> *"**1. Setting the Context** – The process of articulating an institution's objectives and defining its external and internal parameters to be taken into consideration when managing risks.*
> ***2. Risk Identification** – The process of finding, recognizing, and recording risks.*
> ***3. Risk Analysis** – The process of understanding the nature and level of risk, in terms of its impacts and likelihood.*
> ***4. Risk Evaluation** – The process of comparing the results of Risk Analysis with risk criteria to determine whether a risk and/or its magnitude are acceptable or tolerable.*
> ***5. Risk Treatment** – The process of identifying and recommending risk control or Risk Treatment options."*[67]

These steps are then connected to the overall EM approach, as noted in **Figure 8**[68]**.**

It is clear that this is not a methodology for all enterprises, but it is something to be considered if creating a framework based on other methodologies. It may shed light on other aspects of risk assessment that non-federal institutions don't cover, and so will help build a more comprehensive and custom framework for the entity.

[65] Public Safety Canada. p1.
[66] Public Safety Canada. p3.
[67] Public Safety Canada. p4.
[68] Public Safety Canada. p5, figure 1.

Figure 8 - AHRA Process and Linkage to EM Planning



Conclusions

There are many more frameworks not discussed in this report, but the larger, better known frameworks have been discussed. COSO and COBIT are standard frameworks among IT and Internal audit professionals, with emphasis on individuals in the public practice (i.e. ERS, External Audit, IT Audit professionals). It is also important to note that these frameworks are large scale, and may not be effective for all sized companies, and so precautions are to be taken in discussing the use of any of these frameworks and a cost benefit analysis would be encouraged prior to implementation of such large proprortions.

There is general consensus that COBIT is an industry standard for IT Risk guidance. As was noted earlier, this framework is either used, or other frameworks are used that are originally based on COBIT guidelines. This is due to the fact that COBIT is highly integrated with professional standards such as Sarbanes-Oxley Act (SOX)[69]. As an overall internal control framework, COSO is used for the same purposes as COBIT; its integration with SOX[70].

IT risk is not easily assessed or managed, as can be seen with the many frameworks that have been created to do just that. Many of them are either too broad, or too specific, too quantitative, or too qualitative. The organization must first assess its resources to realize how well they can implement and maintain a framework, to ensure that it is most effective; many frameworks do not work due to the user's inability to remain up to date and consistent with the framework. A successful assessment and management framework will allow an enterprise to flourish, minimizing risk and optimizing opportunities for growth.

[69] Institute of Internal Auditors.
[70] Institute of Internal Auditors.

Appendices

Appendix I – Interview with Tony Ha

1. Your current role and qualifications – Senior Consultant – Chartered Professional Accountant, Chartered Accountant, Certified Information Systems Auditor, Certified Information Systems Security Professional

2. What is your exposure to IT risk assessments and management? – COBIT 4.1 in the context of IT Security Process Reviews

3. Frameworks used in past to assess risk? – COBIT 4.1

4. Which have been most effective? – Only had exposure to COBIT 4.1 and COBIT is most commonly used – COBIT 5.0 is current version

- does this differ with department tested? – There are 36 COBIT control objectives and objectives are chosen based on assessed risk and value you're trying to protect

5. In the context of IT risk, what is your opinion on the most effective risk management strategies? – Ensure the concept of a good control is always and consistently applied – Prevent, Detect, Correct

6. How do the ISACA frameworks differ from other assessment frameworks? (Risk IT, COBIT vs. OCTAVE, RMF, FAIR, TARA)

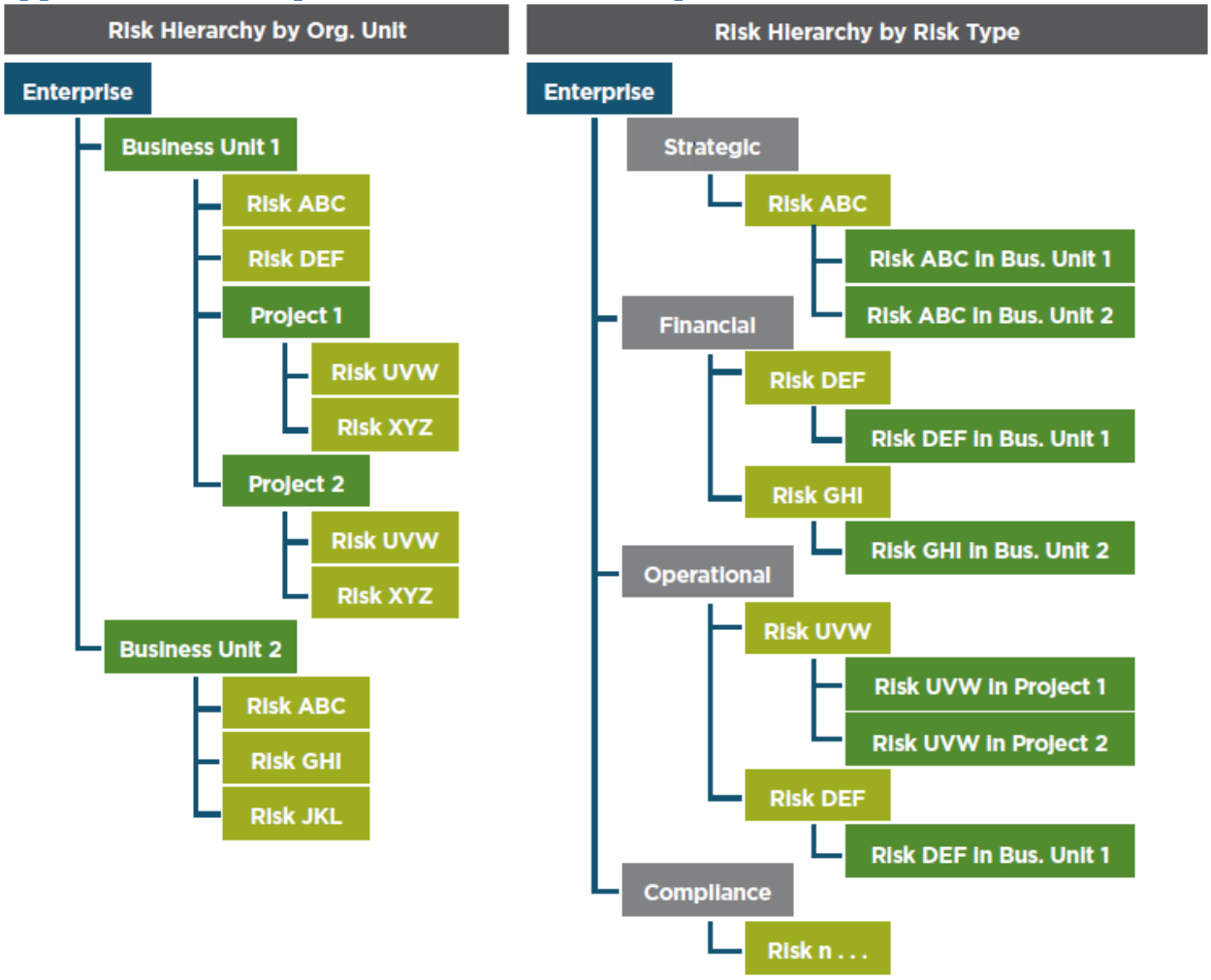
-ISO 27000 – Information Security Management Systems Standards (Standards)

-ITIL – IT Service Management best practices

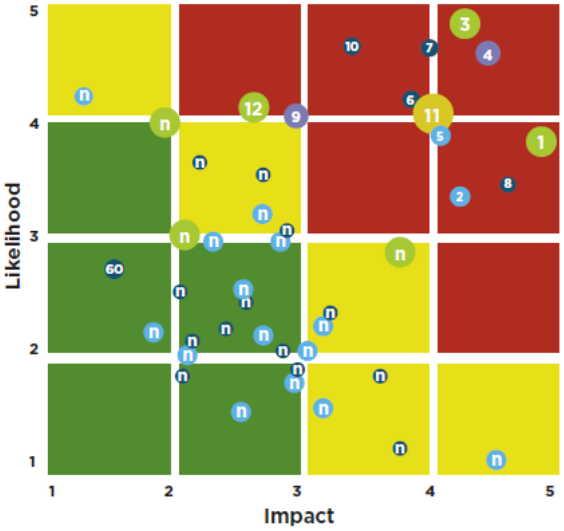
-COSO – comprehensive internal control framework – not just IT and complicated to fully utilize; COBIT is also like a subset of COSO

-Rainbow Series/Books – US Department of Defense Computer Security Standards. Most from the 1980s and 1990s but still considered valuable guidance, even today

Appendix II – Examples of Risk Hierarchies, per COSO



Appendix III – Illustrative Heat Map, per COSO

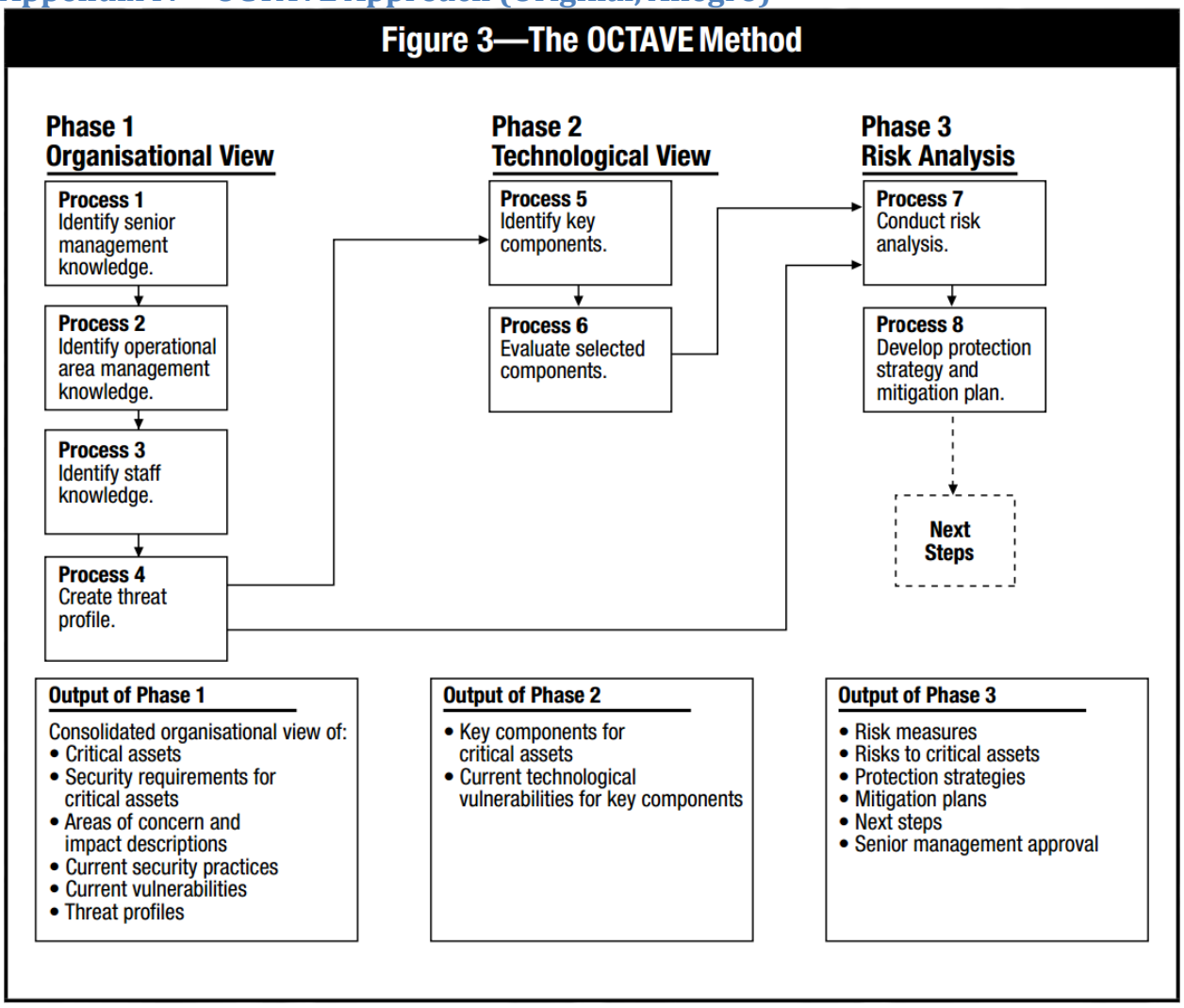


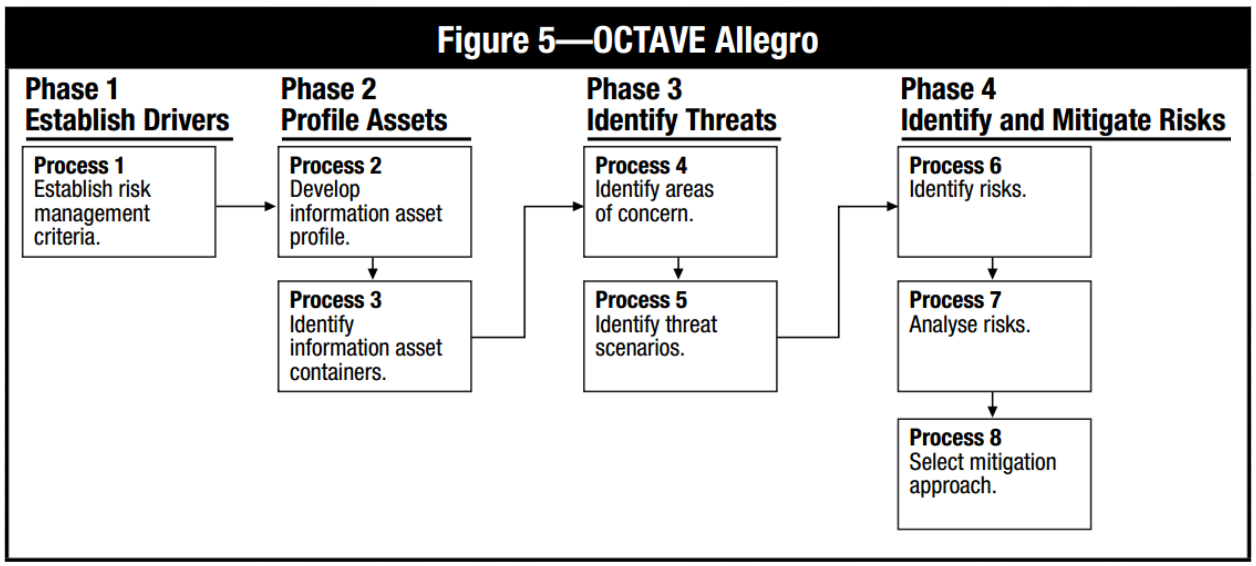
Dots represent risk #1 - #n
Dot size reflects speed of onset:
Very Low Low Medium High Very High

ID	Risk	I	L	V	S
1	Supply chain disruption	4.8	3.7	3.8	4
2	Customer preference shift	4.1	3.3	3.5	2
3	Copper price rise >10%	4.3	4.7	2.3	4
4	Work stoppage > 1 week	4.4	4.5	4.1	3
5	Economic downturn	4.0	3.7	3.5	2
6	Supplier consolidation	3.8	4.2	3.2	1
7	Local competitors enter	3.9	4.5	3.6	1
8	New substitutes available	4.5	3.6	4.2	1
9	Cost of capital rise >5%	2.9	4.0	2.9	3
10	Tighter emission standards	3.4	4.6	2.9	1
11	FCPA violation	4.0	4.0	3.3	5
12	Exchange rate fluctuations	2.7	4.1	2.7	4
n	. . .	...	...	...	...
60	Impairment of assets	1.6	2.7	1.6	1

I = Impact L = Likelihood V = Vulnerability S = Speed of onset

Appendix IV – OCTAVE Approach (Original, Allegro)





Appendix V – Works Cited, and additional sources

Boritz, Jefim Efrim. Computer Control & Audit Guide. 15th ed. Waterloo, Ont.: Centre for Accounting Research and Education, University of Waterloo, 2011. Print.

ISACA. "COBIT5 Introduction." PowerPoint presentation. Web. <http://www.isaca.org/cobit/pages/default.aspx>

COSO. COSO Internal Control -Integrated Framework Update Project Frequently Asked Questions. COSO, Jan. 2012. Web. 3 July 2013. <http://www.coso.org/documents/COSO%20ICIF%20FAQs_January%202012_12%2022%2011.pdf >.

Curtis, Dr. Patchin, Mark Carey, and Deloitte &Touche LLP. COSO: Risk Assessment in Practice. Publication. N.p.: COSO, 2012. Web. <http://www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSO-ERM%20Risk%20Assessment%20inPractice%20Thought%20Paper%20OCtober%202012.pdf>

IBM Global Technology Services. "Supporting information technology risk management – It takes an entire organization." *www-935.ibm.com*. October 2011. IBM. May 29, 2013. < http://www-935.ibm.com/services/multimedia/Supporting_Info_Technology_Risk_Mgmnt.pdf>

Institute of Internal Auditors (IIA). "Common Internal Control Frameworks."Www.theiia.org. IIA, Dec. 2008. Web. 3 July 2013. < http://www.theiia.org/intAuditor/media/images/Burch_dec'08_artok_cx.pdf >.

Intel. "Top 10 Questions for the Threat Agent Risk Assessment (TARA) Methodology."Communities.intel.com. Intel, 20 Aug. 2012. Web. 03 July 2013. < http://communities.intel.com/community/itpeernetwork/blog/2012/08/20/top-10-questions-for-the-threat-agent-risk-assessment-tara-methodology >.

ISACA. "ISACA: Serving IT Governance Professionals." ISACA Issues COBIT 5 Governance Framework. ISACA, 10 Apr. 2012. Web. 27 June 2013. < http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/ISACA-Issues-COBIT-5-Governance-Framework.aspx >.

ISACA. "ISACA: Serving IT Governance Professionals." Risk Assessment. ISACA, n.d. Web. 27 June 2013. < http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx >.

ISACA. The Risk IT Framework Excerpt. Publication. Rolling Meadows: ISACA, 2009. Web. < http://www.isaca.org/knowledge-center/research/documents/riskit-fw-excerpt-8jan09.pdf>

Jordan, Ernest. An Integrated IT Risk Model. Rochester, 2005. ProQuest. Web. 27 June 2013. < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=787326>

KPMG, comp. Defining Issues. Publication no. 13-26. KPMG, May 2013. Web. 3 July 2013. < http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Newsletters/Defining-Issues/Documents/Defining-Issues-O-1305-26.pdf >.

Panda, Parthajit, CISA, CISM, CISSP, PMP. "The OCTAVE® Approach to Information Security Risk Assessment." ISACA Journal 4 (2009): 1-5. Web. < http://www.isaca.org/Journal/Past-Issues/2009/Volume-4/Pages/The-OCTAVE-Approach-to-Information-Security-Risk-Assessment1.aspx>

Rittenberg, Dr. Larry, Frank Martens. COSO: Understanding and Communication Risk Appetite. Publication. N.p.: COSO, 2012. Web. < http://www.coso.org/documents/ERM-Understanding%20%20Communicating%20Risk%20Appetite-WEB_FINAL_r9.pdf>

Spivey, Jeff. "Enterprise Risk Management." Interview by Derek Slater. CSOOnline.com. CSO Magazine, 10 Nov. 2008. Web. 3 July 2013. < http://www.csoonline.com/article/461481/jeff-spivey-on-enterprise-risk-management?page=1>.

Taylor, Hazel, Edward Artman, and Jill Palzkill Woelfer. "Information Technology Project Risk Management: Bridging the Gap between Research and Practice." *Journal of Information Technology* 27.1 (2012): 17-34. *ProQuest.* Web. 27 June 2013. <http://search.proquest.com/docview/918706056/fulltextPDF/13F0D39FB7D3377C4E6/1?accountid=14906>

Trautman, Lawrence James. Threats Escalate: Corporate Information Technology Governance Under Fire. Rochester:, 2012.ProQuest. Web. 27 June 2013. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171026>

Violino, Bob. "IT Risk Assessment Frameworks." CSO. Www.CSOOnline.com, 03 May 2010. Web. 29 June 2013. < http://www.csoonline.com/article/592525/it-risk-assessment-frameworks-real-world-experience >.

Appendix VI – Annotated Bibliography

Author	Title of Article	Periodical/ Website	Vol/No/ Ed	Year Published	Pages	Date Accessed	Location, data base, website, link
IBM Global Technology Services	Supporting information technology risk management	www-935.IBM.com	N/A	2011	8	May 29, 2013	http://www-935.ibm.com/services/multimedia/Supporting_Info_Technology_Risk_Mgmnt.pdf
Annotation A White Paper designed to assist companies on how to identify, balance and mitigate risks in a company. Types of risks are identified, as well as corresponding IT risk management solutions in different areas, such as management/governance, planning/design, etc. Reassessment questions are brought forward to ensure constant maintenance and revaluation of risks occurs. There is a bias to the paper, as it specifies IBM solutions to these IT risks, and it may be limited to the solutions IBM has to offer.							

Author	Title of Article	Periodical/ Website	Vol/No/ Ed	Year Published	Pages	Date Accessed	Location, data base, website, link
Jordan, Ernest	An Integrated IT Risk Model	Papers.ssrn.com	N/A	2005	13	May 27, 2013	ABI Inform
Annotation Jordan makes the point that IT is a significant risk within all other business risks. He first identifies the impacts of IT Risk causes, followed by an understanding of IT risk management. He creates the idea of an IT risk portfolio, wherein the risks are brought together, and none are overlooked; this ensures all impacts of a risk are identified, interrelationships between risks are highlighted and completeness is achieved. Finally, he discusses the role of governance in the IT context and how each player has a responsibility to manage IT risk. A case study and discussion closes out the paper.							

Author	Title of Article	Periodical/ Website	Vol/No/ Ed	Year Published	Pages	Date Accessed	Location, data base, website, link
Karadsheh, Louay A.	A framework for integrating knowledge management with risk management for information technology projects	N/A	N/A	20	214	June 3, 2013	ProQuest

Annotation
The author draws the relationship between knowledge management and risk management for IT projects. Where the majority of the paper discusses background information of IT risk management, as well as includes interviews with industry professionals. The background information within this dissertation will be what is used to back up much of the information related to the data analysis and findings that the author has completed.

Author	Title of Article	Periodical/ Website	Vol/No/ Ed	Year Published	Pages	Date Accessed	Location, data base, website, link
Peltier, Thomas R.	Information Security Risk Analysis	N/A	2nd Ed.	2005	39	May 29, 2013	http://books.google.ca/books?hl=en&lr=&id=n8Z1RDjEKa0C&oi=fnd&pg=PR7&dq=related:_vxwj_Ex054J:scholar.google.com/&ots=S7itsbbA5W&sig=X3-74lt2-an_rZQGTTQIQWwsnlU#v=onepage&q&f=false

Annotation
Basics identified including, but not limited to, why a risk assessment should be conducted, what it covers, who reviews these assessments, and how is success measured. The second portion covers general risk management as part of the business, and employee roles and responsibilities. Risk Assessment steps are highlighted, a cost benefit analysis and risk mitigation are also identified.

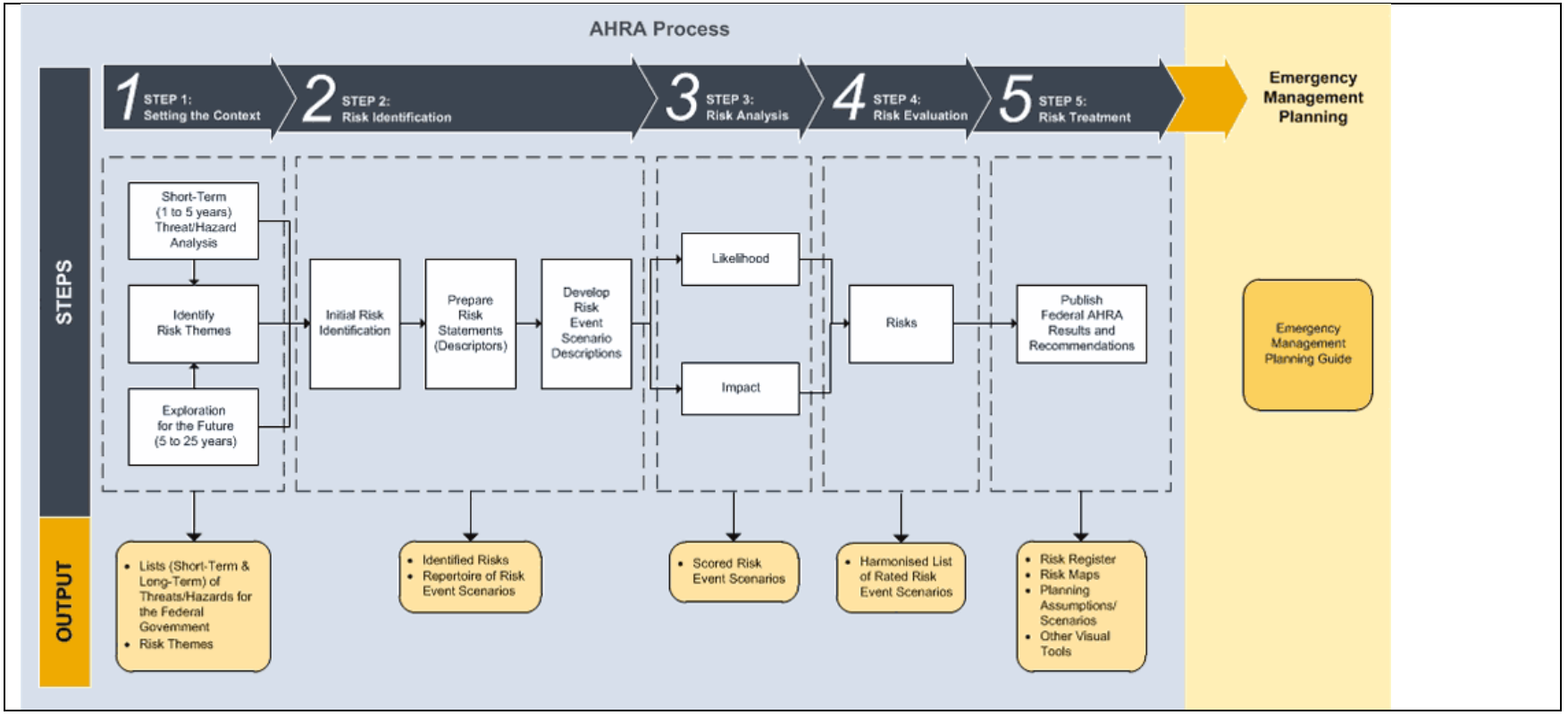
Author	Title of Article	Periodical/ Website	Vol/No/ Ed	Year Published	Pages	Date Accessed	Location, data base, website, link
Public Safety Canada	All Hazards Risk Assessment Methodology Guidelines	www.publicsafety.gc.ca	2012-2013	2012	85	May 29, 2013	http://www.publicsafety.gc.ca/prg/em/emp/2013-ahra/_fl/2013-ahra-eng.pdf

Annotation

As federal institutions are governed under the Emergency Management Act (EMA), they are required to perform an "All Hazards Risk Assessment" (AHRA). What differs with this methodology is the federal focus of risk identification. There are 5 steps, including:

1. **Setting the Context**.
2. **Risk Identification**
3. **Risk Analysis**
4. **Risk Evaluation**
5. **Risk Treatment**

These steps are then linked back to the overall emergency management approach, as displayed below:


AHRA Process
STEPS
1 STEP 1: Setting the Context
2 STEP 2: Risk Identification
3 STEP 3: Risk Analysis
4 STEP 4: Risk Evaluation
5 STEP 5: Risk Treatment
Emergency Management Planning
Short-Term (1 to 5 years) Threat/Hazard Analysis
Identify Risk Themes
Exploration for the Future (5 to 25 years)
Initial Risk Identification
Prepare Risk Statements (Descriptors)
Develop Risk Event Scenario Descriptions
Likelihood
Impact
Risks
Publish Federal AHRA Results and Recommendations
Emergency Management Planning Guide
OUTPUT
Lists (Short-Term & Long-Term) of Threats/Hazards for the Federal Government
Risk Themes
Identified Risks
Repertoire of Risk Event Scenarios
Scored Risk Event Scenarios
Harmonised List of Rated Risk Event Scenarios
Risk Register
Risk Maps
Planning Assumptions/ Scenarios
Other Visual Tools

Author	Title of Article	Periodical/ Website	Vol/No/ Ed	Year Published	Pages	Date Accessed	Location, data base, website, link
Stiennon, Richard	Why risk management fails in IT	Network World	N/A	2012	1	May 29, 2013	ProQuest

Annotation
Lists the reasons why risk management fails in IT, including: Costs and classification, difficulty of value assignment to IT assets, inability of methods to predict disasters, and the devolution of risk management to protect everything. Generally speaking, these are items that companies can use to better their current methods, rather than create or develop a new risk management process.

Author	Title of Article	Periodical/ Website	Vol/No/ Ed	Year Published	Pages	Date Accessed	Location, data base, website, link
Trautman, Lawrence J.	Threats escalate: corporate information technology governance under fire	Papers.ssrn.com	N/A	2012	67	June 2, 2013	ABI Inform

Annotation
Trautman identifies that issues with IT governance are some of the major reasons behind the failure of risk management. The paper attempts make suggestions about the value of the CISO, and there are recommendations to enhance cybersecurity. The author uses present day examples of security breaches, and tries to extract the root cause of each situation. He then follows through with best practice recommendations and how a high level understanding of risks that threaten a company can be managed under an effective crisis management plan.

Author	Title of Article	Periodical/ Website	Vol/No/ Ed	Year Published	Pages	Date Accessed	Location, data base, website, link

USDA	Risk Management Methodology	www.OCIO.usda.gov	Chapter 8, Part I	2012	N/A	May 29, 2013	http://www.ocio.usda.gov/sites/default/files/docs/2012/DM3540-001.htm

Annotation
The USDA created documentation to be followed by companies to create a risk management methodology. Included are responsibilities for different positions, risk assessment background and context, the IT SDLC, and steps to follow to create and maintain a risk assessment model, along with checklist to ensure maintenance of such models. Finally, there are related appendices to ensure the methodology is applied correctly.

Author	**Title of Article**	**Periodical/ Website**	**Vol/No/ Ed**	**Year Published**	**Pages**	**Date Accessed**	**Location, data base, website, link**
Violino, Bob	IT risk assessment frameworks: real-world experience	CSOonline.com	N/A	2010	4	May 29, 2013	www.csoonline.com/article/592525/it-risk-assessment-frameworks-real-world-experience

Annotation
Risk assessment is a big challenge for many organizations, and over the years, there have been many frameworks designed to help identify risk and manage it. Several of these include: Operationally Critical Threat, Asset and Vulnerability Evaluation (**OCTAVE**), Factor Analysis of Information Risk (**FAIR**), the National Institute of Standards and Technology's (NIST) Risk Management Framework (**RMF**), Threat Agent Risk Assessment (**TARA**).