A COMPARATIVE FRAMEWORK FOR EVALUATING INFORMATION SECURITY RISK MANAGEMENT METHODS

W.G. Bornman L. Labuschagne
wgb@adam.rau.ac.za *ll@na.rau.ac.za*

RAU - Standard Bank Academy for Information Technology, Rand Afrikaans University, PO Box 524, Auckland Park 2006, South Africa, April 2004

Abstract: Organisations are under constant pressure from governments and industry to implement risk management methods. There are various information security risk management methods available that organisations can implement, and each has different approaches to identifying, measuring, controlling and monitoring the information security risks. Organisations find it difficult to select an information security risk management method; therefore there is a need for an objective comparative framework to evaluate information security risk management methods. This article provides a comparative framework based on CobiT's Planning and Organisation Control Nine, Assess Risks, which can be used as evaluation criteria for information security risk management methods. Three prominent methods are evaluated using this comparative framework. The evaluated methods' strengths and weaknesses as identified through the comparative framework are highlighted. This comparative framework provides an objective evaluation method to determine whether or not an information security risk management method is in line with information technology governance.

Keywords: Information security risk management, information technology, information technology governance

The financial assistance of the South African Department of Labour (DoL) in this research is hereby acknowledged. Opinions expressed and conclusions arrived at are those of the author and are not necessarily to be attributed to the DoL.

1. INTRODUCTION

Over the last couple of years, information security risk management (ISRM) has become more important for organisations as a result of the release by government and industry governing bodies of risk recommendations or requirements [Cadbury, 1992; King Committee, 2002; Sarbanes-Oxley Act, 2002; The Institute of Chartered Accountants in England & Wales, 1999]. Other pressures to implement solid risk management principles are the increase in high-profile information technology (IT) breaches and the security requirements of technologically integrated business partners.

Currently there are no methods which will assist organisations in determining which ISRM method is the best, in terms of IT governance recommendations, to be employed within an organisation.

This article provides a comparative framework that could be used to evaluate different ISRM methods. This comparative framework can indicate an ISRM method's alignment with best practice as recommended by an internationally accepted IT governance framework.

An internationally accepted IT governance framework is identified and a comparative framework developed from its recommendations. This article illustrates the usability of the comparative framework by comparing three ISRM methods. Subsequently, the results of each methodology's evaluation are discussed. Only three ISRM methods are used in the illustrations, as the evaluation serves to display the practical implementation and value of the comparative framework.

2. DEVELOPING AN APPROACH TO COMPARE ISRM METHODS

The selection and implementation of an ISRM method is tasked to the tactical and, in some instances, the operational level of an organisation by the governing body of that organisation. The governing body, like the board of directors, is held accountable for any actions within the organisation [King Committee, 2002; Sarbanes-Oxley Act, 2002] and "sponsors" the risk management requirements.

The strategic level recommendations and requirements can be regarded as the requirements criteria for evaluating different ISRM methods. ISRM falls within the IT governance scope [IT Governance Institute, 2000], and therefore an acceptable IT governance framework, method or approach will serve as the basis for the comparative framework. IT governance is the procedures, protocols, requirements and guidelines that recommend IT implementation within an organisation [IT Governance Institute, 2000].

Organisations must ensure that the ISRM methodology employed is in line with international best practice, as government regulations regarding privacy [Baker and McKenzie, 2004] can impact ISRM accountability and trading partners can require secure and reliable electronic communication. Although best practice frameworks and recommendations exist, a method must ensure that best practice is translated into processes and steps. The comparative framework must embody the recommendations of the information security assessment process of an internationally accepted IT governance framework.

An internationally accepted IT governance framework, and the one that is used, is the CobiT Framework [IT Governance Institute, 2001]. CobiT serves as the starting point of the comparative framework as illustrated in figure 1 below.

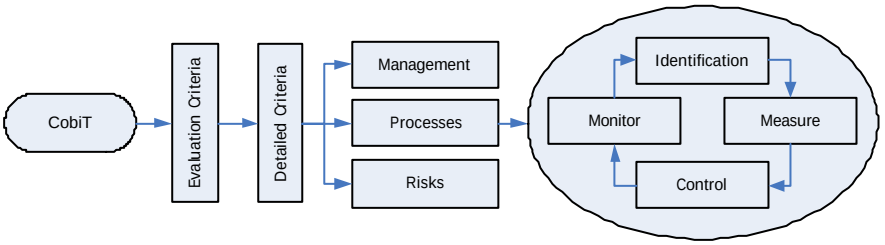

Figure 1: Comparative Framework

2.1 Why CobiT?

CobiT can be used as a declaration of criteria for specific audit outcomes [IT Governance Institute, 2000]. CobiT is based on international best practice from various countries, including the United States of America, Europe, Australia, Canada and Japan; therefore it serves as a more than appropriate framework on which the comparative framework can be based [IT Governance Institute, 2002]. Because of CobiT's global implementation, it is a generic framework which enables it to be implemented in various industries. CobiT assists organisations in bridging the gap between business risks, technical issues and requirements of controls.

2.2 What is CobiT?

CobiT (Control Objectives for Information and related Technology) is an IT governance framework. The third and most recent edition of CobiT was released in July 2000 by the Information Systems Audit and Control Foundation, and the IT Governance Institute. CobiT consists of various products: the Executive Summary, Implementation Toolset, Management Guidelines, Framework, Detailed Control Objectives and Audit Guidelines. Most of these products set out controls, their implementation and control guidelines in four groupings or domains: they are Planning and Organisation, Delivery and Support, Acquisition and Implementation, and Monitoring.

With each new edition of CobiT, the framework has evolved from an internal and external assessment tool to a management tool for maturity programs, and with the introduction of the third edition, to an IT governance and risk management framework [Pritchard, Da Veiga, KPMG, 2003].

CobiT was used in developing the comparative framework. The next section describes the process that was followed in developing the comparative framework.

3. EVALUATION CRITERIA

In developing the comparative framework, the approach that was taken started with a review of the CobiT products. The Executive Summary, Management Guidelines, Framework, Implementation Toolset and Detailed Controls were reviewed. A single control was identified that directly addresses the assessment of risk. This control is the Planning and Organisation Control Nine, Assess Risks.

A list of recommendations was compiled from the various areas within each CobiT product. Each product contains distinctive areas, for instance Considerations, Enablers and Business Requirements. These distinctive areas were all considered in the development of the comparative framework. The list of recommendations was then logically grouped into three categories. The three categories answer the questions: what should be done, by whom (including responsibilities) and how should it be done? The three categories are:

1. Risks (What?) – This category contains all the criteria of the comparative framework that relate directly to the elements of risk.
2. Management (Who/Responsibility?) – The management grouping addresses those aspects of the risk management process for which management is responsible.
3. Processes (How?) – The assessment of risk is a process that has to be completed. These processes are categorised as four generic steps: identification, measurement, control and monitoring.

The comparative framework focuses on recommendations at business level rather than at technical operational level.

CobiT is an extensive document with control objectives that address different IT areas within an organisation. For the purposes of this article the single control (Planning and Organisation Control Nine) is sufficient, as the scope of the comparative framework is limited by the article. It would be possible to develop criteria for other IT areas, for instance procurement, by basing them on the different CobiT objectives.

The next section provides detail on the comparative framework that was developed.

3.1 Detailed Criteria

This section provides detailed descriptions of each component of the comparative framework. Some of the components that were identified were duplicated in several of CobiT's products. These duplicates were reconciled and are represented by a single component. The component descriptions are grouped according to the three categories discussed above.

3.1.1 Risks

- Different Kinds of Risk – A distinction will have to be made between the different risk sources and the kinds of risks. Kinds of risks refer to the groupings such as regulatory, technological and continuity.
- Defined Risk Tolerance Profile – Each organisation is willing to accept a certain level of risk which is indicated by the risk tolerance profile. The profile provides an indication of the actions that should be taken with regard to risks, for instance which level of risk should be accepted or managed.
- Risk Action Plan – This plan will have to identify the risk strategy which will include the actions of how the organisation will accept risk, or control or mitigate risk through cost-effective controls.

3.1.2 Management

Management is responsible for establishing a systematic risk assessment framework. The framework as discussed in Planning and Organisation Control Nine (Assess Risks) of the control objectives describes various aspects that should be incorporated. The following criteria form part of the aspects that should be included:

- Defined Risk Process Ownership / Responsibility and Risk Accountability – Risk management requires a specific process owner. This owner will be responsible for all the processes and actions comprising the risk management method. Certain organisations require that a risk committee be put in place, due to the size of the organisation, to be responsible for specific areas of risk management, but a single individual should ultimately be responsible within an organisation. A distinction will have to be made between risk responsibility and risk accountability. According to the King II Report [2002] and the Sarbanes-Oxley Report [2002], the board is accountable although the responsibility can be delegated down within the organisation.
- Risk Management Improvement Project – ISRM methods will have to include improvement projects. The improvement projects refer to the continuous evaluation and bettering of the risk management processes. The method will have to facilitate training and brainstorming sessions and workshops.

- Policies and Procedures – Policies and procedures are the formal documentation of the organisational risk culture. These policies and procedures will dictate how risks should be managed at different levels within the organisation.
- Support Documents – Support documents are required to assist in the third-party assessment of the risk management process as well as the facilitation of risk monitoring, the setting of risk limits and evaluation of control effectiveness. Other supporting documents will also have to serve as input for the risk management methods; these documents include business risks, operations and IT risk assessment documents.
- Reassessments – Risks are ever-changing and new information security risks are introduced on a daily basis. Therefore, structured risk reassessments will have to be done. The methods will have to be able to comply or recommend a reassessment schedule. Updates of risk limits should form part of risk reassessment. Management will have to ensure that reassessments are catered for.
- Global and System Level Assessments – The ISRM method will have to facilitate assessment at system and global levels. System level is the hardware and software level within an organisation, while global level includes assessments that are not directly attributed to the system. Global level will include the affect humans and external elements can have on the system.
- Management Input – Management requires timely and accurate information to direct the organisational strategies in the long run. Therefore, the ISRM method will have to facilitate the input of top management.
- Risk Strategy – The ISRM method will have to employ a strategy that will avoid, mitigate or accept risks.

3.1.3 Processes

Risk management, irrespective of organisational level or industry, follows certain risk management steps. Various risk management methods have different steps that vary in number and scope. However, when considering the Plan, Do, Check and Correct (PDCC) processes described within CobiT, generic risk management steps can be identified. They are Identify, Measure, Control and Monitor. Each of the evaluation criteria is described within the sub-groupings of the processes.

3.1.3.1 Identification

- Cause and Effect Relationships – During the risk identification step the causes of the risks will have to be related to the effect that they could have on the organisation. In other words, the effects that a risk will have on the organisation will have to be linked or mapped to the cause.
- Examine Essential Elements of Risks – CobiT regards the essential elements of risk to include tangible and intangible assets, asset value, threats, vulnerabilities, safeguards, consequences (impacts) and likelihood of threat.
- Considerations – IT and its security component are not and do not exist in a closed system. They are affected by and affect other items and events, so when identifying risk there are other areas that have to be considered. CobiT regards the following risk areas as important: Business, Regulatory, Technology, Trading, Partner and Human resources.
- Updated Risk Limits – Risks as well as the ability of an organisation to accept risks are ever-changing. Therefore risk limits have to be updated on a regular basis.
- Acceptance of Residual Risks – Organisations can never afford to address all risks; the remaining risk is referred to as residual risk. The residual risk also includes the risks that the organisation is willing to accept according to its determined risk appetite or tolerance. A

process has to be in place to formally accept the residual risks. This process will have to include any measures the organisation takes to address the risks.
- Risk Acceptance of Organisation – This refers to the measurement of the ability or level of risk an organisation can accept before controlling or mitigating the risks. These measures will be used in the organisational risk profile.

3.1.3.2 Measure

Quantitative or Qualitative Measures – When measuring risk of an organisation, two different measurements can be assigned to a risk. The first is a quantitative measure. Quantitative measures can be any numerical value, for instance a cash value, server down time or loss of revenue. A qualitative measure is a relative value assigned to a risk, for instance high, medium or low.

3.1.3.3 Control

- Risk Ranking – Risk ranking is the process in which the risks are ranked according to the organisational specification, for instance the most likely risks or the risks with the highest impact. The ranking of risks can be either quantitative or qualitative in nature.
- Third Party Objectivity – Organisations employ the services of independent third parties to verify specific functions within the organisation. Organisational risk controls and processes will have to be of such a nature to assist with any third party validation.
- Return on Investment (ROI) Calculations – ROI is a calculation that indicates to management the "usefulness" of their investments. IT risks are unfortunately of such a nature that quantitative measures are rarely possible.
- Control Balance – Cost-effective controls should be balanced between the following four control types: Preventive, Detective, Corrective and Recovery.
- Control Integration (Control Conflict Management) – Some controls might conflict with others, for instance a firewall that blocks all but Internet-related communication ports and causes a proprietary communication program to malfunction, which in essence is a denial-of-service risk. A process to identify and manage any conflicting controls will have to be present.
- Control Purpose Communication – The purpose of the controls has to be communicated to relevant parties, such as employees. For instance, the need for passwords will enable employees to have control over the use of information stored on the workstation.

3.1.3.4 Monitor

- Facilitate the Monitoring of Controls – The cost-effective controls that are implemented will have to be monitored. Monitoring of the controls can include automated monitoring.
- Incident Reporting Processes – Incidents can constitute negative or positive events. For instance, a hacking attempt that was prevented by an implemented control can provide just as much information about the risk action plan as a successful hacking attempt.
- Improved Project Feedback– Once shortcomings in the risk action plan have been identified, it has to be improved. Feedback is essential to ensure that the necessary actions are taken.
- Maintained Risk Information – CobiT is a framework that facilitates the auditing of risk controls. Any information gathered regarding risk identification, measurement, control implementation, monitoring, processes, procedures and protocols must be documented and maintained in a structured manner.

3.2 Standardised checklist

The comparative framework's components described above provides the organisation with a standardised checklist to compare ISRM methods with international best practice. The next section describes the process used in evaluating three current ISRM methods.

4. COMPARISON PROCESS

The majority of ISRM methods are proprietary with very little publicly available information apart from marketing literature. Often organisations do not have the available capital to purchase different ISRM methods in order to evaluate them. Therefore, the evaluation process was based on documentation obtained through printed material, presentation software, demonstration server platforms or Internet published material. The material was reviewed within the comparative framework against the criteria as indicated in Appendix A.

5. ISRM METHOD COMPARISON

Three ISRM methods were identified. They are the CCTA Risk Analysis and Management Method (CRAMM), version 5, the CORAS methodology for model-based risk assessment and the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method, version 2.0. Following is a brief overview of each.

5.1 CORAS

CORAS [Bjørn, 2002] is a model-based risk assessment method and is a research and technological development project under the Information Society Technologies (IST) programme. Ten companies and research institutions made up the project consortium.

CORAS's goal is to adapt, refine, extend and combine methods for risk analysis. Some of the methods employed include Event-Tree-Analysis, Markov, HazOp and FMECA.

The CORAS methodology is a risk management process based on the standardised modelling technique UML. Different standards such as the AS/NZS 4360:1999 "Risk Management" and ISO/IEC 17799-1: "Code of Practice for Information Security Management" and the Reference Model for Open Distributed Processing (RM-ODP) were used in the development of the risk management process.

During 2003 a CORAS Risk Assessment Platform was made available to the public. This platform includes user guidelines, the CORAS methodology documentation, an assessment repository and a reusable elements repository.

5.2 OCTAVE

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) was developed by the Carnegie Mellon Software Engineering Institute (SEI). The core elements of OCTAVE are criteria which organisations can use to develop their own methodology. Although various methods can be developed that fulfil the set criteria, the OCTAVE method was developed to fully comply with the OCTAVE criteria. Although the OCTAVE method was developed for large organisations, a method known as OCTAVE-S was also developed for smaller organisations. Like the OCTAVE method, it is freely available.

The basic premise of OCTAVE is structured interviews at various levels within the organisation to identify critical assets and then determine the risks to those assets.

5.3 CRAMM

CRAMM (CCTA Risk Analysis and Management Method) was developed by the CCTA (Central Computer and Telecommunication Agency) in 1985. The CCTA was tasked by the UK Government Cabinet's Office to investigate the risk analysis and management methods within the central government for IT. Subsequent to the investigation, it developed CRAMM, which drew on existing best practice.

CRAMM is currently in its fifth version, which was released by Insight Consulting in 2003. This version also provides compliance guidance on the BS 7799 standard, part two.

CRAMM provides steps to determine the likelihood and the impact of a threat on an asset. Subsequently, these determined values are used to calculate the risk value for each threat to all the assets. CRAMM also provides a "fast-track" method by logically grouping assets.

6. ISRM METHOD RECOMMENDATION

The evaluation of the three ISRM methods, as illustrated in Appendix A, has indicated that they are all very strong in the first two categories (Risk and Management). However, the Processes category, especially the control and risk monitoring processes, has been identified as an area that is lacking according to the comparative framework.

Each of the evaluated ISRM methods has its strong and weak elements. This section will describe the strong and weak areas of each method as has been highlighted by the comparative framework outlined above.

6.1 CORAS

The information used for the evaluation process is part of the CORAS Risk Assessment Platform which utilises XML (Extensible Mark-up Language) and is a Java application server-based platform. The platform includes all the documentation required to install and operate the software, as well as detailed documentation regarding the CORAS methodology.

The CORAS methodology documentation is separated into three levels: basic, decision and full. The documentation of each of these three levels was examined during the evaluation process.

The evaluation indicated that CORAS does not provide for risk management improvement projects that are facilitated by workshops/meetings and employee training. The lack of a reassessment schedule and updating of risk limits indicates that the CORAS methodology serves as an initial risk assessment method but does not provide for an iterative risk assessment approach, as supported by the lack of risk monitoring which forms part of the evaluation category processes.

CORAS does not explicitly specify the identification of existing safeguards or controls. This method further lags behind in the controls section of the process evaluation category.

One of the strongest elements of CORAS is the Lesser General Public Licensed software. This software is freely available and does not require a major capital expenditure.

The identification process has to consider various risk areas, for instance business risks, regulatory risks and trading risks. Due to CORAS's nature of utilising different risk assessment methods, the consideration of other risk areas will depend on the selected risk assessment method.

CORAS provides for countermeasures but does not facilitate return on investment (ROI) calculations or deliver a distinctive balance between preventive, detective, corrective or recovery controls. No control integration management processes are in place or processes for assessing the effectiveness of the controls. There is no formal procedure for accepting residual risks. CORAS facilitates third party control objectivity through documentation.

6.2 OCTAVE

Information used during the OCTAVE evaluation process was obtained from published literature [Alberts and Dorofee, 2002] and OCTAVE Criteria as published by the Carnegie Mellon University and CERT [Alberts and Dorofee, 2001].

One distinctive feature of OCTAVE is the assessment of risk without taking into consideration the probability of a threat realising.

As with the other two methods, OCTAVE fulfils all the criteria for the Risk category.

OCTAVE facilitates the development of a reassessment schedule, and provide for the update of risk limits during the risk assessment processes. When the risk strategy is defined, OCTAVE only takes into consideration the mitigation and acceptance of the risk, but not its avoidance.

Two areas need mention regarding the identification process. OCTAVE does not utilise quantitative risk ranking, but quantities can be used in determining the qualitative scale according to which risks are ranked and measured. The various risk areas that have to be considered are not directly addressed, unlike the regulatory and technology risks. The other risk areas are indirectly considered by the interviewees when determining the impact a threat can have on the organisation.

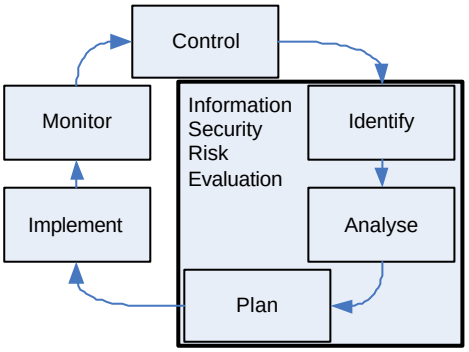

Figure 2: OCTAVE Method

OCTAVE is a risk management method that focuses only on identifying, measuring and providing a plan for managing risk (Figure 2), so the control and monitor criteria would seem to be areas that would not favour OCTAVE. However, OCTAVE highlights the need for control purpose communication and recovery control selection. Figure 2 indicates that OCTAVE has more steps than the generic steps highlighted in the comparative framework. These additional steps were taken into account during the evaluation process. Where possible , the additional steps were incorporated in the generic steps, but disregarded where this was not practical.

Although the method does not provide concise steps for monitoring the risk plan, the method recognises the importance of the monitoring process. The two criteria that OCTAVE fulfils are the improvement project feedback and structured risk information maintenance.

6.3 CRAMM

CRAMM's evaluation information was based on the CRAMM V Walkthrough and Overview Flash Presentation provided by Insight Consulting [Insight Consulting].

CRAMM fulfils all the criteria of the Risk category. It takes into consideration different risk categories, has a defined risk tolerance profile and has a risk action plan.

This ISRM method does not assist in risk management improvement projects. Therefore, no training, meetings or workshops are utilised in this regard. CRAMM does not take into consideration any risk supporting material such as business, operational and IT risk assessment documentation. Reassessment schedules and the updating of risk limits do not form part of the CRAMM methodology. With regard to the risk strategy, only the mitigation of risks is addressed. The risk strategy is not in terms of risk avoidance or acceptance.

The identification stage of the processes is a very strong area of CRAMM. It takes into consideration all the different elements of risk, the tangible and intangible assets, threats, asset values, safeguards, consequences and the likelihood of threats. CRAMM has a cause and effect relationship through a threat-asset based relationship. Other risk area considerations depend on the intended use of the method. CRAMM can be implemented for system development, policy development and compliance, reviewing security aspects, compliance audits, continuity and contingency planning, among other things.

CRAMM utilises qualitative and quantitative measures. The method does not identify the risk acceptance capacity of an organisation.

The control process of CRAMM fares better than the other two methods against the criteria. Third party objectivity is facilitated through the BS7799 part two compliance facility built into the CRAMM V software. CRAMM does not directly facilitate the calculation of return on investment on risk controls; however, the implementation of controls should be based on value to the organisation. There are four shortcomings of CRAMM's control process. CRAMM does not have a control integration process in place and does not communicate the purpose of controls. It does not facilitate the monitoring of control effectiveness and does not put controls in place for residual risks. CRAMM does not update the risk limits, nor does it provide an incident reporting process.

7. METHOD LIMITATIONS

The comparative framework and process taken to evaluate ISRM methods is by no means flawless and has some limitations.

- ISRM methods such as OCTAVE have the ability to be customised to organisational needs. This ability can result in certain processes being excluded during the implementation of that particular methodology. The comparative framework does not take into consideration the customisation of a methodology.
- When organisations undertake ISRM, certain business and practical considerations are taken into account. These considerations include the estimated cost, time and resources required. The comparative framework and process do not take these considerations into account as they are very subjective in nature and differ between organisations.
- The comparative framework and process do not take into consideration the organisation's scope statement and motivation for implementing ISRM. For instance, organisations might want only to identify and measure their risk without controlling or monitoring it.

- According to CobiT, the risk strategy of an organisation should be in terms of avoidance, mitigation and acceptance. Another consideration, which CobiT does not refer to, could be the transfer of a risk. Transferring risk refers to shifting the burden or responsibility of a risk to a third party [Standards Australia, 1999]. The transfer of risk is usually when the likelihood of a threat is low and the threat's impact relatively high.

8. CONCLUSION

This article presents a comparative framework based on the internationally accepted CobiT IT governance framework. Because the comparative framework is based on this internationally accepted IT governance framework, it is an objective method of comparing different attributes of ISRM methodologies. The comparative framework also provides an indication of whether or not an ISRM method is in line with IT governance recommendations.

The comparative framework was used to evaluate three current ISRM methods. These methods were CRAMM, OCTAVE and CORAS. Subsequent to the evaluation, each of the methods revealed its strengths and weaknesses. Important aspects regarding ISRM methods came to light during this evaluation.

Although the methods relatively complied with the Risks and Management groupings, the Monitoring and Controlling processes of risks are lacking in all the evaluated ISRM methods. The methods do not strike a balance between different types of controls, they do not have control integration management and do not institute residual risk controls. During the risk monitoring process the methods lack formal incident reporting processes.

Another important area that is lacking is the reassessment of risks. None of the methods have a formal reassessment schedule recommendation and two methodologies neglect to update risk limits.

Further research should be undertaken into striking a better balance between risk controls, and developing better incident reporting processes and control integration management within ISRM methods.

This comparative framework enables organisations to evaluate various ISRM methods without purchasing the methods. The comparative method provides organisations with a means of comparing ISRM methods based on published and/or non-commercial information and ensuring that their methods are in line with IT governance recommendations.

The practical illustration of the comparative framework highlighted that there is still research potential in aligning ISRM methods with IT governance best practice recommendations.

REFERENCES

Alberts, C.J. & Dorofee, A.J. (June 2001). *OCTAVE Method Implementation Guide Version 2.0*. Carnegie Mellon University.

Alberts, C.J. & Dorofee, A.J. (June 2002). *Managing Information Security Risks – The OCTAVE Approach*. Pearson Education Ltd.

Baker & McKenzie. *Global E-Commerce Law – Canada Security Legislation and Regulations*. Available from: http://www.bmck.com/ecommerce/canada-s.htm#161 (Accessed 11 January 2004).

Baker & McKenzie. *Global E-Commerce Security Law – US Federal Security Legislation and Regulations*. Available from: http://www.bmck.com/ecommerce/fedlegis-s.htm (Accessed 11 January 2004).

Bjørn, A.G. (January 2002). *CORAS, A Platform for Risk Analysis on Security Critical Systems – Model-based Risk Analysis Targeting Security.* Presented at EWICS Symposium 22.01.2002. Available from: http://www.nr.no/coras (Accessed August 2003).

Cadbury,. The Committee on the Financial Aspects of Corporate Governance and Gee and Co. Ltd. (1992). *The Financial Aspects of Corporate Governance*. Gee.

Dimitrakos, T., Ritchie, B., Raptis, D. & Stølen, K. (2002). *Model Based Security Risk Analysis for Web Applications: The CORAS Approach.* EuroWeb 2002.

Insight Consulting. (2003). *CRAMM Expert Walkthrough and Overview – Flash Presentation.*

IT Governance Institute. (2001). *Board Briefing on IT Governance*. Available from: http://www.ITgovernance.org

IT Governance Institute. (July 2000). *CobiT 3rd Edition*. The CobiT Steering Committee and the IT Governance Institute.

King Committee on Corporate Governance. (2002). *King II Report – 2002.* Institute of Directors (IOD), South Africa.

Labuschagne, L. (2003). *Utilising the OCTAVE Methodology to Your Advantage by Reducing Information Security Risk and Vulnerability*. Proceedings of the IT Risk Management Symposium (South Africa). Conducted by the Institute for International Research.

Parker, D.B. (2000). *Why the Due Care security review method is superior to Risk Assessment.* The Newsletter for Information Protection Professionals, Number 212, November 2000. Computer Security Institute.

Pritchard, S., Da Veiga, A. & KPMG International. (2003). *CobiT – The New Frontier*. Proceedings of the IT Risk Management Symposium (South Africa). Conducted by the Institute for International Research.

Sarbanes-Oxley Act of 2002. (23 January 2002). United States Congress. (H.R. 3763).

Standards Australia. (1999). *Risk Management – AS/NSW 4360:1999*; Standards Australia/Standards New Zealand.

The Institute of Chartered Accountants in England & Wales. (September 1999). *Internal Control – Guidance for Directors on the Combined Code.*

Appendix A: Evaluation Criteria

✔ – Fulfils Criteria ✘ – Does not fulfil Criteria ? – Depends on Other Factors	CRAMM	OCTAVE	CORAS
Risks			
Defined Categories of Risk	✔	✔	✔
Defined Risk Tolerance Profile	✔	✔	✔
Risk Action Plan	✔	✔	✔
Management			
Defined Risk Ownership and Responsibility	✔	✔	✔
Risk Management Improvement Project	✘	✔	✘
Training	✘	✔	✘
Meetings/Workshops	✘	✔	✘
Risk Assessment Policies and Procedures	✔	✔	✔
Risk Support Documents	✘	✔	✘
Business Risks/Operational Risk/IT Risk Assessment	✘	✔	✔
Reassessment Schedule	✘	✔	✘
Global and System Level Assessment	✔	✔	✘
Management Input	✔	✔	✔
Identify Risk Strategy in terms of Risk			
Avoidance	✘	✘	✔
Mitigation	✔	✔	✔
Acceptance	✘	✔	✔
Processes			
Identification			
Cause and Effect Relationships	✔	✔	✔
Examines Essential Elements of Risk			
Tangible Assets	✔	✔	✔
Intangible Assets	✔	✔	✔
Threats	✔	✔	✔
Asset Values	✔	✔	✔
Vulnerabilities	✔	✔	✔
Safeguards	✔	✔	✘
Consequences	✔	✔	✔
Likelihood of Threat	✔	✔	✔
Considers			
Business Risk	?	?	?
Regulatory Risk	?	✔	?
Technology Risk	?	✔	?
Trading Risk	?	?	?
Partner Risk	?	?	?
Human Resource Risk	?	?	?
Updated Risk Limits	✘	✔	✘
Measures Risk Acceptance Capacity of Organisation	✘	✔	✔

	CRAMM	OCTAVE	CORAS
Measurement			
Qualitative Measure	✔	✔	✔
Quantitative Measure	✔	✘	✔
Control			
Risk Ranking			
Qualitative	✔	✔	✔
Quantitative	✔	✘	✔
Facilitates Third Party Objectivity	✔	✘	✔
Controls Facilitate ROI Calculations	?	✘	✘
Strikes Balance Between -	✘	✘	✘
Prevention	✔	✘	✘
Detection	✔	✘	✘
Correction	✔	✘	✘
Recovery	✔	✔	✘
Control Integration (Control Conflict Management)	✘	✘	✘
Control Purpose Communication	✘	✔	✔
Process for Formal Acceptance of Residual Risk	✔	✘	✘
Residual Risk Controls	✘	✘	✘
Risk Monitor			
Facilitates the Monitoring of Controls	✘	✘	✘
Incident Reporting Process	✘	✘	✘
Improvement Project Feedback	✔	✔	✘
Maintained Risk Information	✔	✔	✘