Risk Management Practice Guideline

Risk Management Task Force
February 2007

Forward

This is the first CIPS (Canadian Information Processing Society) best practice. It has been developed to support the IT professional in discharging her[1] responsibility to assess and manage IT risks. It is presented as a Practice Guideline. This means that the IT professional has a responsibility to generally understand the material in this Guideline, but is free to exercise her professional judgment in deciding how this Practice Guideline applies in her work.

NOTE: A Practice Guideline is the least restrictive Best Practice (or Practice Standard) that may be imposed on the IT professional. It requires the IT professional to generally familiarize herself with the Practice Guideline, but recognizes that application will vary considerably and no special justification is required to deviate from the Practice Guideline. A Recommended Practice imposes the same requirements as a Practice Guideline and requires that the IT professional provide justification for deviations from that practice. Finally, a Required Practice imposes the same requirements as a Recommended Practice and requires that all exceptions to the practice be supported by a thorough justification.

[1] We follow the convention of using the feminine version of the third person singular pronoun. Please read this as “her or his”, “she or he”, etc.

Participants

This practice guideline was prepared by a special Risk Management Task Force of the Canadian Information Processing Society. The working group consisted of the following members:

R. Fabian, *Chair*

K. Augustine	P. Bassett	B. Bey
J. Boufford	E. Brown	C. Carbno
V. Chiew	J. Finch	S. Ibaraki
J. Muir	G. Smith	M. Sullivan
	A. Todd	

Table of Contents

1 Executive Summary

The IT professional should begin every assignment assessing the possible risks associated with that assignment. The level of detail and the degree of rigor in that assessment will vary. At a minimum, the IT professional should informally review possible risks and their likely impact. The IT professional has a responsibility to communicate her findings to management and to any people reporting to her.

Within the established risk management policies and practices of the organization employing her, the IT professional should follow appropriate best practices to manage the risks that have been identified. This Guideline recognizes that risk management best practices will vary. Specifically, different risk management best practices are appropriate for system development, system acquisition, and system delivery. And some degree of tailoring will be required before any pre-existing best practices can be effective in a particular organization.

COBIT[1] is used as a general IT governance framework. It places risk management within a context, providing general answers to questions about how risk management relates to the other important IT processes. A simplified risk management activity flowchart is adopted from COBIT. It identifies five key risk management activities.

This Guideline does not provide direct answers about how the IT professional should best identify, assess, or manage risk. It points to published best practices that can be consulted. Which best practices to consult will depend on the organization and the work to be performed. The Canadian Risk Management Guideline for Decision-Makers, the COSO material on risk, and COBIT are offered as best practices to consult regarding high-level risk management policies and practices.

The key ISO/IEC/IEEE risk management standard (16085) is offered as a best practice to consult regarding risk management during the full system life cycle. The risk management material from the Software Engineering Institute , the US Air Force, the Defense Acquistion University, and the Spiral Model are offered as best practices to consider for risk management during development and acquisition.

ISO/IEC 20000 and ITIL are offered as best practices to consider during service delivery and service support. ISO/IEC 17799 and the ENISA material are offered as best practices to consider in connection with risks association with system security. And, finally, PMBOK and Prince2 are project management best practices that include useful material on project risk management.

2 Introduction

CIPS has accepted, in principle, that the IT professional has a responsibility to assess and manage IT risk. This guideline explains what this means for the IT professional. It should be viewed as a Practice Guideline – IT professionals have a responsibility to be generally familiar with this material and should apply it selectively in all of their professional work.

The challenge for any IT Risk Management Guideline is the multi-faceted nature of risk. Specifically:

- There are a large number of established risk management best practices.
  - Terms are defined differently
  - Scope is defined differently
  - Activities are defined differently
- Different organizations view risk differently
  - Some want to manage for success, not worry about failure
  - Some have established risk management policies and practices
  - Some are open to improving their risk management practices
- Different individuals have differing scope to manage IT risks
  - The project manager should manage project risks
  - The operations manager should manage operational risks
  - The CIO should establish risk management policies and practices

Under these conditions, a “one size fits all” guideline is neither good theory nor good practice. What the responsible IT professional should do to assess and manage IT risks will depend on the organization within which they are working and on the role they play within that organization. This document provides a guideline to help the IT professional decide what is required of her in discharging her responsibility to assess and manage IT risks.

CIPS online Risk Management information will, over time, become an important resource in helping IT professionals understand how their responsibility to assess and manage risk is best discharged. It is intended that a growing range of risk management case studies be available as well as additional information about best practices to consider. An online Risk Management forum will be an interactive resource to provide information and advice to IT professionals about the risk management challenges they face. As a first step in providing this information, CIPS has established an IT Risk Management Wiki.

3 Risk Definition

Risk arises because something may occur – an event – which leads to business outcomes other than the planned ones. It's important to understand both the probability of the event occurring and the resulting gap between planned and realized outcomes. The Risk Severity is then (Probability of Event) x (Outcome Gap).

Most of the systems risk literature concentrates on events leading to a failure to achieve planned outcomes. The primary focus is on reducing threats or reducing their impact. The financial risk literature takes a more positive view and examines events which may have a positive as well as a negative impact on planned outcomes.

This guideline concentrates on risks with a negative impact, but recognizes that leading organizations may be ready to consider risks having a potential positive impact. This Practice Guideline encourage the consideration of both positive and negative risks, but recognize that many organizations will only be ready to consider risks that have a negative impact.

4 Professional Responsibility

CIPS has accepted that:

IT professionals have a responsibility to assess risks before each assignment.
and
IT professionals have a responsibility to manage risks during assignments.

What this means in practice will depend on a number of factors. How much overall responsibility has the IT professional been given? How much importance does the organization attach to assessing and managing risks? What are the risk tolerance and risk appetite of the organization and of IT group within the organization?

At a minimum, the IT professional should examine the risks she faces before undertaking any professional IT assignment. This requires both identification of possible risks and a determination of the likely impact of each such risk. The IT professional should follow through, taking such action as is acceptable to the organization to manage risks. Further, the IT professional should hand to her successor an organized view of any remaining risks.

The IT professional may not be empowered, or allowed, to expend all of the resources that she believes would be required to fully manage risk. But she still has a basic professional obligation to communicate her findings about assessment of risk to management and to any staff that may be working for her.

5 The Individual's Role

For most IT professionals, IT is a collective undertaking. People in IT work together to deliver value to the organization that employs them. Individuals may exercise a measure of independent professional judgment, but all of their work takes place within an organizational context. The organization establishes the polices and practices under which work in IT is performed.

The individual IT practitioner may have only limited influence over the organization's risk management policies and practices. The IT professional has some responsibility to "manage" risk, but what should she do if the organization does not have the policies or practices in place that allow risks to be effectively managed? Specifically, what happens if the organization is not prepared to have its IT professional spend sufficient time to effective managing risk?

Under almost all conditions, it's good IT professional practice to begin assignments by first taking some time to identify risks and determine their possible impact. This may be a brief exercise, conducted informally, during the first hours that the IT professional is on their new job. But it's unprofessional to walk into a new assignment without some appreciation for the risks facing you.

The IT professional has a further obligation to communicate her risk findings. She should discuss the risks in her assignment with both the person to whom she reports and any people who may report to her. What happens next will depend on the organization for which the IT professional works, and on the nature of her assignment.

Under the "best" conditions, the IT professional will be given the resources required to appropriately assess and then manage risk, and be given the support to effectively discharge their risk management responsibilities. Under all conditions, the IT professional will pay attention to risk, taking such appropriate risk management actions as may be allowed by their organization. The IT professional has a responsibility to communicate to her successor an organized view of any remaining risks.

6 Risk Framework

Risk management has been a central concern of the financial industry for more than a century. Risk management has been elevated to a Board level concern by recent legislation and regulation in Canada and internationally. Risk management is accepted as a basic project management responsibility. IT risk management has been addressed by several different best practices, some accepted as standards, others accepted as useful practices.

COBIT[1] provides a useful IT governance framework that allows risk assessment and risk management to be placed in context. COBIT is the most widely employed IT Governance best practice standard. It divides IT into 34 processes, one of which is "Assess and manage IT risks". Other COBIT processes include: Manage quality; Manage projects; Ensure systems security; Enable operation and use; and Procure IT resources. COBIT puts IT risk management in the context of all of the processes required to deliver IT.

COBIT offers some other important advantages:

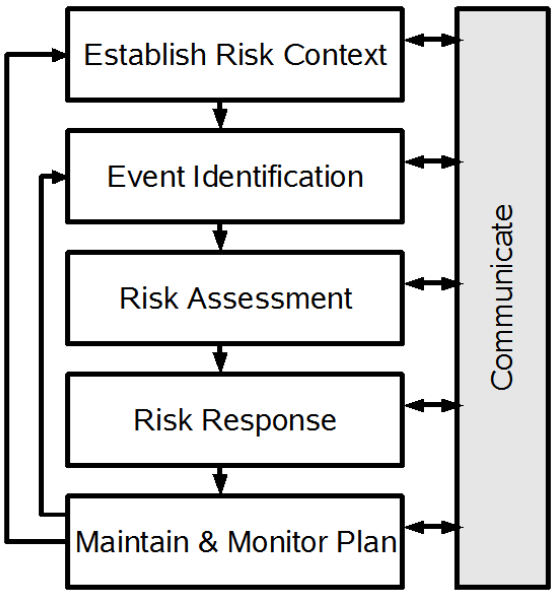
COBIT's sponsors are working actively to harmonize COBIT with other widely used IT best practices, specifically with COSO[2], ITIL[3], ISO 17799[4], and PMBOK[5].
COBIT defines a maturity model for the "Assess and manage IT risks" process – users are not confronted with a single monolithic standard.
COBIT defines a RACI (Responsible, Accountable, Consulted, Informed) chart that provides a useful, first cut determination of who should be doing what.
COBIT breaks down "Assess and manage IT risks" into six more Detailed Control Objectives:
    IT and Business Risk Management Alignment
    Establishment of Risk Context
    Event Identification
    Risk Assessment
    Risk Response
    Maintenance and Monitoring of a Risk Action Plan

COBIT recognizes that tailoring will be required to modify its best practices to fit what will be appropriate for any specific situation.

COBIT is accepted by this Practice Guideline as defining the risk management context. It should be consulted to determine the basic relationship between risk management and all of the other activities that are important to IT. Further, this Practice Guideline recommends that the Risk Management Glossary developed by ENISA[6] be used as the source for the definition of specific risk management terms.

7 Risk Activity Flow

There are many risk management activity flowcharts. Somewhat different terms are used and the activity breakdown is not always the same. This Practice Guideline will generally follow the COBIT activity model. The model to be followed can be represented in the following flowchart.



NOTE: COBIT identifies the importance of "IT and Business Risk Management Alignment". This activity is clearly important for effective IT Governance. It will significantly inform "Establish Risk Content". The alignment activity is viewed as being outside the relatively narrow view of risk management adopted by this Practice Guideline.

7.1 Communicate

The risk management literature is clear and unequivocal. Communication up, down, and sideways is critical to effective risk management. The IT professional has a responsibility to communicate risk information to management and to her team. Beyond that minimum requirement, it is often useful to communicate risk information more widely to a number of concerned stakeholders. An important aspect of the need to communicate is the need to communicate to any successors.

7.2 Risk Context

The organization and its IT group will have in place risk management policies and practices. These broad risk management policies and practices, or their relative absence, will guide the development of any specific Risk Response Plan. The particular activity under review will also contributed to determining exactly how the Risk Response Plan is to be developed. This activity based

concern can be viewed as the micro level context for development of the Risk Response Plan.

7.3 Identify Risks

There are several broad approaches that can be taken to identify risks. Some combination of these approaches will normally be adopted.

- **Judgment** – Individuals or groups follow a process aimed at helping them identify those unplanned events which put the ability to meet objectives at risk.
- **Scenarios** – Qualitatively different alternatives are examined. Often used to examine corporate strategies and their associated risks. Particularly useful in the face of possible discontinuities.
- **Model** – A model is developed for the activities under review with a view to mathematically identifying risks. Used widely in financial industry, but only selectively in the IT industry.
- **Check List** – A check list or taxonomy of possible risks is examined to identify the risks facing the activities under review. Can be a useful starting point, but some customization is almost always required.

7.4 Assess Risks

For each event giving rise to a risk, a probability must be determined, and likely impacts identified. In the special case where numerical values can be assigned to this probability and where the impact can have a numerical value, the Risk Severity will have an explicit numerical value. It is often impossible to attach meaningful numbers to the probability or the impact. Under such a condition, a more qualitative approach is appropriate. Probability and risk may be assessed as high, medium, or low, with a resulting severity calling for immediate action, careful planning but no immediate action, or only careful monitoring.

7.5 Risk Response

Four general approaches have been employed to respond to events that threaten achieving the organization's objectives.

- **Tolerate Risk (acceptance)** – The organization may decide that it will just tolerate the risk. Often this will happen when the consequences are relatively easy to tolerate, or the cost of doing anything meaningful about the risk is too high.
- **Transfer Risk (sharing)** – This is what insurance providers have traditionally offered. The challenge in any effort to transfer or share risk is to make sure that entity to whom the risk is being transfer is both ready and able to assume that responsibility.
- **Reduce Risk (reduction)** – This requires that the activity giving rise to

the risk be changed to reduce the risk or that other actions be taken which will reduce or counter balance the risk.

- **Eliminate Risk (avoidance)** – Typically this will require that the organization avoid performing the activity which gave rise to the risk. This is not a widely applicable response – any valuable activity will give rise to some risk. Risk is a necessary part of action.

7.6 Maintain & Monitor Plan

A Risk Response Plan has been developed. The Plan, including its response to events (immediate or contingent actions) and control activities are approved and the recommended responses are owned by the managers responsible for any affected processes. Once the Plan has been in place for some time, events will have occurred, and risks will have been faced. The quality and value of the Plan needs to be reviewed to determine if any changes in the Plan are required. Should any changes be required, the process would cycle back to a reidentification of risks, reassessment of risks, and modification of the Risk Response Plan. The experience with individual Risk Response Plans should be cycled back to refine, and improve the organizational Risk Context.

8 Best Practices

There are a very large number of "best practices" that could be used in connection with risk management. This is not intended to be an exhaustive list of best practices that warrant consideration. It does contain many of the more important practices that the IT professional should consider. To be included on this list, there must not be any license to use the practice, but there may be a fee to obtain a copy of the document describing the best practice.

A four-way distinction provides a useful way to view possible best practices:

Governance – The organization has a responsibility to set risk management policies and practices. The absence of any explicit risk management policies does not necessarily mean that there are no risk management practices in the organization. The IT professional with senior IT management responsibilities should concern herself or himself with establishing appropriate risk management policies and practices. Best practices to consult:

- CAN/CSA-Q830-03 Risk Management: Guideline for Decisions-Makers[7]
- COSO Enterprise Risk Management - Integrated Framework (Executive Summary)[2]
- COBIT version 4.1, specifically "Assess and manage IT risks"[1]

Development – The typical concern is with a system development project. Many projects fail to deliver the expected benefits, within the planned time and cost limits. There can be a real gap between planned and realized outcomes. Considerable work has been done on how to best manage risk on system development projects. Best practices to consult:

- ISO/IEC 16086:2006 Information technology - Software life cycle processes - Risk Management[8]
- US Air Force, Software Technology Support Center, Guidelines for Successful Acquisition and Management of Software-Intensive Systems, specifically the chapter on Risk Management[9]
- Software Engineering Institute, Taxonomy-Based Risk Identification, and subsequent Technical Reports on Risk Management, 1993 (CME/SEI-93-183)[10]
- Software Engineering Institute, Spiral Development: Experience, Principles, and Refinements, 2000 (CMU/SEI-2000-SR-008)[11]

Operations – Organizations can be at considerable risk from problems arising in operations. Changes are not properly tested or installed. Capacity is not adequate to meet demand. Security has been compromised by parties who attack an organization's systems. There is a growing literature on how to best protect systems operations.

- ISO/IEC 20000-1, Specification for Service Management[12] and ISO/IEC 20000-2, Code of practice for Service Management[12], Standards developed in connection with the ITIL library of best practices[3]
- ISO/IEC 17799:2001 Information technology - Code of practice for information security management[4]

European Network and Information Security Agency, Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools, 2006[6]

Acquisition – More and more systems and system services involve a significant acquisition activity. Outsourcing is one obvious example, but so are the growing number of applications that are purchased rather than being developed internally. Systems acquisition is different and requires a different approach to risk management.

Risk Management Guide for DOD Acquisitions[13]

Other - Project Management must address risk management questions. Both the North American PMBOK (Project Management Body of Knowledge)[5] and the UK/European Prince2 (PRojects IN Controlled Environments[14]) provide useful best practices for project management. Both provide guidance on risk management best practice for project managers.

9 Related Practices

Any process that will deliver value will have some associated risk. Improving predictabiliy (reducing risk) at a cost of delivering reduced value can be a bad trade-off. The IT Governance Institute (author of COBIT) has recognized the fundamential importance of delivering value – its Val IT framework [15] provide useful guideance for how to improve value delivery. Nothing in this Practice Guideline should be interpreted as denying the fundamental importance of value delivery.

There are hundreds of best practices that cover different aspects of IT, and different activities with significant IT components. Many of these best practices address risk related concerns. This Practice Guideline explicitly considers the ITIL[3] and ISO 20000[12] best practices for service delivery and service support; the security best practices found in ISO 17799[4] and ENISA[6]; and the PMBOK[5] and Prince2[14] best project management practices. All of these best practices have some relevance to the IT profesisonal's risk management responsibilities.

In addition to these explicity identified best practices, the IT professional also has a responsibility to familarize herself with the other best practices that may be relevant to her activities or to the domain of application within which she is working.

10 References

[1] COBIT – COBIT is the most widely accepted IT Governance best practice. It has been developed by the IT Governance Institute (www.itgi.org) and is now in version 4.1. Copies are available after free registration on the IT Governance Institute website.

[2] COSO – The US savings and loan crisis in the 1980s gave rise to the Committee of Sponsoring Organizations of the Treadway Commission. Its best practices have been accepted as meeting Sarbanes-Oxley requirements. COSO has published several useful risk management documents, specifically "Enterprise Risk Management Framework – Integrated Framework". (www.coso.org)

[3] ITIL – The Information Technology Infrastructure Library was developed by the UK Government and is being maintained by the UK's Office of Government Commerce (OGC) and the IT Service Management Forum International. ITIL is widely used as the source of best practices in service delivery and service support. ITIL materials are available in Canada from itSMF Canada (www.itsmf.ca).

[4] ISO/IEC 17799 – This is the most widely accepted international collection of best practices for IT security. There is an associated recommended practice for IT security – ISO/IEC 27001.

[5] PMBOK – The Project Management Institute (www.pmi.org) has developed the Project Management Body of Knowledge. The most recent version was published in 2004 and includes a full chapter of project risk management. PMI offers the Project Management Professional (PMP) certification.

[6] ENISA – The European Network and Information Security Agency have published a useful Inventory of Risk Management/Risk Assessment Methods and Tools. It can be found at: www.enisa.europa.eu . They have also develop a useful Glossary for risk management.

[7] CAN/CAS Q850 – Canada has been an active participant in the development of risk management guidelines for decision makers. The guideline is relatively high level, but does provide a uniform context for all risk management activities.

[8] ISO/IEC 16086 – The is the international standard version of the Software Lifecycle Risk Management standard developed by the IEEE. This places risk management within the accepted international software lifecycle model (as described in ISO/IEC 12207 and ISO/IEC 15288).

[9] US Air Force – The US Air Force has developed and makes freely available a useful "Guidelines for Successful Acquisition and Management of Software-Intensive Systems". It is available in both a condensed version (2003) and an expanded, original version (2000). Included in both versions are useful and practical chapters on risk management.

[10] SEI Taxonomies – The Software Engineering Institute located at Carnegie-Mellon University has published several risk management taxonomies. It published "Taxonomy-Based Risk Identification" (CMU/SEI-93-TR-6) in 1993, and more recently published "A Taxonomy of Operational Risks" (CMU/SEI-2005-TN-036).

[11] Boehm Spiral Model – Barry Boehm first described a Spiral Model for system development in the 1980s. Work has continued on the model. It's now required for US DOD system development and acquisition. One useful reference is a report published by the SEI "Spiral Development - Building the Culture" (CMU/SEI-2000-SR-006).

[12] ISO/IEC 20000 – The British Standards Institute developed a Service Management Specification and a Service Management Code of Practice. They have become ISO/IEC 20000-1 and ISO/IEC 20000-2. In typical application, the ITIL family of best practices is used to define the processes in 20000-2.

[13] Risk Management Guide for DOD Acquisition – The US Department of Defense has established a Defense Acquisition University (www.dua.mil). This Risk Management Guide can be found on the Defense Acquisition University website.

[14] Prince2 – In addition to ITIL, the OGC is also responsible for maintaining the Prince2 project management methodology. It defines a specific approach to managing projects, with full attention being paid to risk management during project life cycle.

[15] Val IT – The IT Governance Institute is in the process of developing and publishing material on it Val IT Framework. The initial documents appears in 2006, and more are expected in the near future. This is a value focused framework that exists in parallel with the COBIT control / governance focused framework.

11 Reference Websites

cve.mitre.org/
A list of standardized names for vulnerabilities and other information security exposures - CVE aims to standardize the names for all publicly known vulnerabilities and security exposures.

www.dau.mil/
The Defense Acquisition University (DAU) is the one institution that touches nearly every member of the DoD Acquisition, Technology, and Logistics (AT&L) workforce throughout all professional career stages.

www.comp.glam.ac.uk/Teaching/ismanagement/riskman1f.htm
The best are good at reducing risk through risk management ... consider why we should manage risk ...define and discuss ways of thinking about risk

www.rmahq.org/RMA/
Member driven organization focusing on risk management in the financial services industry. Includes a bookstore, journal, certification information, ...

en.wikipedia.org/wiki/Risk_management
Traditional risk management focuses on risks stemming from physical or legal ... Financial risk management, on the other hand, focuses on risks that can be ...

www.sei.cmu.edu/risk/index.html
The main page for SEI risk management. ... Software Risk Evaluation | Continuous Risk Management Guidebook Risk Process Check

www.rma.usda.gov/
Links and information about the Federal Crop Insurance Corporation (FCIC) that helps farmers survive a major crop loss. The RMA also provides training to ...

www.nonprofitrisk.org/
Provides risk management assistance and resources for community-serving nonprofit organizations. Many articles and tutorials.

www.irmi.com/
A research and publishing company focused on risk management and insurance. Site includes articles on various risk management topics, online CE courses, ...

www.rims.org/
Not-for-profit professional international association. Provides a career center, educational courses, annual conference, discussion groups, directory of ...

www.managementhelp.org/risk_mng/risk_mng.htm
Risk management often focuses on matters of insurance. ... Safety / Slips and Falls :

Risk Management Internet Services Library (rmis.com) ...

www.rmmag.com/
Once again in 2006, risk management was at the forefront of many of the year's top ... Risk and Insurance Management Society (RIMS) · 1065 Avenue of the ...

opim.wharton.upenn.edu/risk/
Research, publications, projects, working papers, conferences.

www.sra.org/
The Society for Risk Analysis (SRA) provides an open forum for all those who are interested in risk analysis. Risk analysis is broadly defined to include ...

www.riskworld.com/
Resources on risk assessment and risk management in medicine, environment, and society at large.

www.theirm.org/
Non-profit organization dedicated to providing risk management related education. Includes diploma information, career center, events calendar, ...

www.baz.com/kjordan/swse625/index.html
We are a group of dedicated software professionals committed to increasing the knowledge of risk management ...

www.rspa.com/spi/project-risk.html
R.S.Pressman & Associates - Risk Management Resources; Risk Management Tutorials, Articles and Papers; Risk Tools; Books

www.tbs-sct.gc.ca/pubs_pol/dcgpubs/riskmanagement/siglist_e.asp
Government of Canada - Risk Management - Policies and Publications

www.nr.no/~abie/RiskAnalysis.htm
An index to: Risk Analysis, Risk Assessment, Risk Management

www.baz.com/kjordan/swse625/index.html
dedicated software professionals committed to increasing the knowledge of risk management and general software project management skills

February 2007