Enterprise Risk Management (ERM) Guideline

contact:
Edward Robertson, MPA, CRM
Manager, ERM
Risk Management Branch
595 Pandora Ave., Victoria BC
PO Box 9405 Stn Prov Govt V8W 9V1
Tel: (250) 356-5833
Fax: (250) 356-6222
Edward.Robertson@gov.bc.ca
Government of British Columbia  
Risk Management Branch – Enterprise Risk Management (ERM) Guideline

TABLE OF CONTENTS

Foreword: Audience; How to use this Guideline.  
ERM Process Model

1 BACKGROUND: BC GOVERNMENT ERM PROGRAM

1.1 BC GOVERNMENT ERM PROGRAM
   1.1.1 Definition of ERM
   1.1.2 ERM for Government: Program and Vision
   1.1.3 Benefits and Outcomes

1.2 IMPLEMENTATION
   1.2.1 General Advice
   1.2.2 Implementation Styles: BC Public Sector and Lessons Learned
   1.2.3 Getting Started
   1.2.4 Frequently Asked Questions

1.3 RISK CULTURE
   1.3.1 Introduction: Sensitive Risk Information
   1.3.2 Risk Information Contradicting Executive Direction
   1.3.3 Risk information as Potential Political Embarrassment
   1.3.4 Freedom of Information Requests
   1.3.5 Risk-Aversion versus Risk-Tolerance
   1.3.6 Recommendations and Resources

1.4 RESOURCES
   1.4.1 Internet Resources
   1.4.2 BC Government InTRAnet Resources
   1.4.3 Glossary

2 APPLICATION OF ENTERPRISE RISK MANAGEMENT PROCESS

2.1 COMMUNICATE AND CONSULT
   2.1.1 Consultative Team Approach
   2.1.2 Initial Planning

2.2 ESTABLISH THE CONTEXT
   2.2.1 Context Analysis 1: to Inform a Risk Management Plan
   2.2.2 Context Analysis 2: to Prepare for a Risk Identification Session
   2.2.3 Specialized Contexts: Sub-disciplines within Risk Management

2.3 IDENTIFY RISK
   2.3.1 Risk Identification Methods
   2.3.2 How to State Risks
2.4 ANALYZE RISK
   2.4.1 Risk Analysis Matrix: Likelihood, Consequence, Ranking
   2.4.2 Inherent vs. Residual Risk
   2.4.3 Advice on Assigning Likelihood & Consequence

2.5 EVALUATE RISKS
   2.5.1 Risk Evaluation Means a Finer Assessment
   2.5.2 Existing Controls; Tolerance; Action

2.6 TREAT RISKS
   2.6.1 Diversity of Risk Treatment (Mitigation)
   2.6.2 Ensuring Effective Risk Treatment (Mitigation): Advice for Facilitator

2.7 MONITOR AND REVIEW
   2.7.1 Monitor: Regular Management of Risk Information
   2.7.2 Review: Historical Risk Information

2.8 RECORD THE RISK MANAGEMENT PROCESS
   2.8.1 Summary: Documentation of ERM
   2.8.2 Risk Register
FOREWORD: AUDIENCE; HOW TO USE THIS GUIDELINE

This Guideline is intended for BC government ministry and provincial public sector employees having Enterprise Risk Management (ERM) responsibilities. It gives recommended practices to apply the AS/NZ standard in public sector settings. It can be used in conjunction with other sources as follows:

1. **AS/NZS 4360:2004** ("standard") 28-page generic risk management model; The present Guideline is adapted from this standard.

2. **HB 436:2004** ("Handbook") is the AS/NZS reference for those who have a grasp of the basics, but want to explore interpretive materials and use them “in the context of their own environments... to develop their own specific risk management approaches”.

Fig.1 The ERM Process Model from AS/NZS 4360:2004
1 BACKGROUND: BC GOVERNMENT ERM PROGRAM

1.1 BC GOVERNMENT ERM PROGRAM

1.1.1 Definition of ERM
Risk management is defined as “the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects” (AS/NZS 4360:2004, p.4).

Enterprise Risk Management (ERM) signifies: 1) the management of risk not only in conventional hazard categories, but in the full spectrum of strategic and operational risk; and 2) the adoption of risk management throughout the organization. It is essentially a decision process for managing uncertainties, and gives policy and resource allocation decisions a defensible basis.

The ERM process, as defined by the AS/NZ standard (see Fig.1, page 3) is generic. It is equally viable to manage risk in, for example, finance, where the uncertainties of credit, market, and liquidity are quantifiable, and in programs where only qualitative information is available.

The diagram in Fig. 2 illustrates the ERM process with typical examples under each heading. Note that disciplines like emergency and business continuity planning are specific treatments (mitigations) within a wider process.

Fig.2 The ERM Process in the Public Sector (adapted from AS/NZS 4360:2004).
### 1.1.2 ERM for Government: Program and Vision

The ERM program was begun April 01, 2002 with the inclusion of ERM in corporate policy (Core Policy Manual Chapter 14) and adoption of the Australia-New Zealand model as the government standard. The vision of the program is to achieve a mature culture of Enterprise Risk Management in government and the broader provincial public sector, where “risk management is an integral part of strategic and business planning” and risk information is communicated both within the organization and to stakeholders. (ref: Risk Management Maturity Model). The program elements are illustrated in Fig.3.

ERM for government has three major aspects. One is the progress that ministries and public sector agencies are currently making in discovering the value of risk analysis in service planning, projects, programs and policy development. The second is risk management at a government-wide, strategic level, with senior executive providing leadership – this aspect is under development by Risk Management Branch. The third is the cultural shift anticipated whereby the excessive risk-aversion typical of bureaucracy is replaced by responsible risk taking and evidence based decision-making.

---

#### Fig.3. ERM Program for BC Government and Broader Provincial Public Sector

**Enterprise–wide Risk Management for BC Government and the Broader Provincial Public Sector**

<table>
<thead>
<tr>
<th>REGULATORY / ADMINISTRATIVE FRAMEWORK</th>
<th>ORGANIZATIONAL CAPACITY- BUILDING</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROVINCIAL LEGISLATION</td>
<td>CLIENT NEEDS ANALYSIS</td>
</tr>
<tr>
<td></td>
<td>Government Risk Culture Surveys</td>
</tr>
<tr>
<td></td>
<td>AWARENESS</td>
</tr>
<tr>
<td>CORPORATE POLICY</td>
<td>Executive Presentations</td>
</tr>
<tr>
<td>Core Policy Manual Ch14</td>
<td>ERM Community of Practice</td>
</tr>
<tr>
<td>Capital Asset Management Framework</td>
<td>TRAINING</td>
</tr>
<tr>
<td>BC Auditor General Reporting Principles</td>
<td>ERM Training Courses</td>
</tr>
<tr>
<td>CORPORATE STANDARD</td>
<td>CONSULTING SERVICES</td>
</tr>
<tr>
<td>AS/NZS 4360:2004</td>
<td>Risk Management Branch Consulting and Advisory Services</td>
</tr>
<tr>
<td>BEST PRACTICES</td>
<td>COMMON TOOLS and RESOURCES</td>
</tr>
<tr>
<td>ERM Guideline</td>
<td>Risk Register Standard Template</td>
</tr>
<tr>
<td>Risk Dictionary</td>
<td>ERM InTRANet and Internet Web Pages</td>
</tr>
<tr>
<td>RISK MATURITY MODEL</td>
<td></td>
</tr>
<tr>
<td>COMMON PLANNING and REPORTING INSTRUMENTS</td>
<td></td>
</tr>
<tr>
<td>Service Plans; Annual Reports; etc.</td>
<td></td>
</tr>
</tbody>
</table>
1.1.3 Benefits and Outcomes

The immediate benefit of ERM is having a structured process to support decision-making. Policy, plans, and program design are defensible when consistent with a comprehensive risk profile that is informed by the organization’s goals and values.

Planners can effectively integrate expert opinion and stakeholder views, expressed as discrete risks. Spending priorities, as well as previously hidden overspending (excessive controls) are brought to light. This helps government move away from excessive risk aversion, and towards evidence-based decisions. Positive outcomes have been demonstrated in BC and other jurisdictions.

ERM Community of Practice members in BC Government ministries have commented on the confidence inspired by capturing all critical business problems in risk analysis:

- “The discipline in applying the model set the stage for in-depth discussion”;
- “Risk analysis puts more rigour into the process... When you have all the critical issues framed and quantified...this makes your recommendations much harder to refute” (Ministry of Health);
- “The initial risk assessment was the right thing to do and it definitely helped to focus the project work” (Ministry of Transportation);
- “This was the first time that the whole set of issues had been articulated, with key stakeholders assembled, in a structured manner” (Ministry of Children and Family Development).

The risk process outlined in this guideline has been applied in, for example: Crown Contaminated Sites Program (Ministry of Environment); Safe Drinking Water Program (Ministry of Health); Land Use Planning policy (Office of the Premier); Ministry Service Plan (Ministry of Forests); and organization-wide strategic and operational planning (Camosun College). In all cases, appropriate mitigation strategies increased the likelihood of program relevance, efficacy and successful implementation.

The UK National Audit Office report “Managing Risks to Improve Public Services” (22 October 2004) describes benefits of ERM in government operations, including better delivery of public services through improved efficiencies, and support for innovation.

Case histories in the UK government have shown the efficacy of analyzing risks of disruptions to service delivery. In complex “high reliability” operations, where consequences of failure are severe, stakeholders meet to share previous experience and develop robust risk analyzes.

The Management Advisory Board of the Australian Public Service has, similarly, observed the following outcomes for ERM:

- More effective delivery of government programs;
- More effective allocation and use of resources;
- Higher standard of customer service & accountability;
- Greater exercise of creativity and innovation in management practice;
- Improved capacity to manage in the face of competing obligations; and
- Improved agency morale.
1.2 IMPLEMENTATION

1.2.1 General Advice

The Core Policy Manual Chapter 14 states that each ministry is “accountable to Treasury Board for developing, implementing and maintaining an Enterprise-wide Risk Management process”.

There is no single correct way to do this. Essentially, it is a matter of:

- interpreting the ministry’s or agency’s business to determine where there is significant uncertainty regarding priorities or range of outcomes;
- proving the value of risk analysis in pilot sessions; and
- integrating risk management into regular strategic and operational planning.

It is scarcely possible to obtain value by doing risk management as a scripted compliance exercise. Let us assume that the potential benefits of risk management are understood. In that case, we assert that public servants must take the initiative to interpret their organizational context to determine needs, be creative in applying the method, and maintain awareness of a continually shifting risk environment. Consider:

- executive’s and staff’s perceptions of risk in relation to their business;
- the risk management practices and culture already extant; and
- the degree of formalized risk management infrastructure desired.

The Conference Board of Canada report entitled “Risk Management: Moving the Framework to Implementation” (February, 2004) is an international study of lessons learned in early stages of ERM implementation. It refers to varied approaches, and includes three crucial recommendations:

- Adapt and learn: Develop and refine the implementation process through experimentation, real organizational learning, and the engagement of staff and stakeholders;
- Provide leadership support; and
- Integrate into management processes: Incorporate risk management into existing planning and decision-making processes. (Emphasis added).

Literature on program implementation is clear in defining conditions for the success of a new management technique. These include senior executive leadership, and staff support through involvement in proving the concept. Phased implementation allows for feedback and improvement.

1.2.2 Implementation Styles: BC Public Sector and Lessons Learned

BC public sector entities’ implementation styles of ERM comprise a spectrum, ranging from initial project activity to relatively sophisticated practice.

Many government offices, especially in specialized scientific or engineering disciplines, already manage risk in some way, whether their methods are quantitative or qualitative, highly structured or informal. ERM embraces established practice in managing risk.
Many ministries, agencies, health authorities, etc., have carried out risk assessments for plans or programs on a one-off basis. Camosun College went beyond this and successfully integrated risk analysis into regular management planning, using a project manager as a temporary risk champion. In a more formal approach, Chief Risk Officers have been established in, for example, the Ministry of Employment and Income Assistance and BC Hydro.

Lessons learned can be summarized as follows:

- The ERM process serves as a framework against which to check existing risk assessment practices for completeness;
- Risk analysis applied to major public policy development, program design, partnerships, outsourcing and other initiatives can demonstrate the process and prove its value;
- The “champion” (person or group) plays an essential role to initiate ERM and adapt it to the organization; and
- New positions including Chief Risk Officer and a committee structure are not essential, but can provide visible leadership for a formal approach.

Drawing upon BC government experience, we suggest it is appropriate to plan ERM implementation considering the following criteria:

a) the ways in which ERM can potentially add value, that is, “ensure that a culture of active, explicit and systematic risk management exists, where well managed risk taking is fully encouraged and supported, and where decisions are routinely based around accurate and well informed judgements about risk.” (NAO, ibid.);

b) the focus of risk analysis (e.g., strategic or service plan, programs or projects);

c) the type and extent of risk management already practiced, and the ways in which ERM methodology might help to make it complete;

d) the degree of formalized structure (e.g., new positions or committees) desired;

e) training required in facilitation skills and ERM; and

f) the pattern of communication of risk information desired.
1.2.3 Getting Started

Assuming that executives have already endorsed the adoption of ERM or a trial, a champion or facilitator will likely have the responsibility for implementation. While advanced facilitation skills are useful, anyone capable of chairing a meeting should be able to gain the cooperation of participants to experiment with risk analysis using this Guideline.

Initial ERM activities consist of the following steps:

a) Interpret the business needs, and establish the organizational context for risk management: Consult with internal stakeholders to arrive at a common understanding of priorities for risk analysis. Determine the logical starting point for ERM. Consider integrating risk analysis with service or project planning.

b) Coordinate initial risk identification and analysis sessions: Determine roles and responsibilities and pilot the following:
   - adapt the standard risk register with appropriate columns;
   - facilitate risk identification session (or do some alternate method of capturing risk, such as interviews) and analysis;
   - record results and feed mitigations back into action plans;
   - monitor follow-up action.

c) Plan the consistent capture and communication of risk information. Assess the information management and reporting needs.

d) Use an incremental approach; build participants’ review and feedback into the design.

(See also section 2.2.1 Context Analysis 1: to Inform a Risk Management Plan)

1.2.4 Frequently Asked Questions

• "Where do we start?"
  Introduce ERM where it will add value in solving critical business problems. Test your approach in manageable steps. Risk analysis of, for example, the service plan, can benefit executives and operational staff as they articulate and exchange views of risk. Similarly, various stakeholders can begin to understand one another’s business by cooperating to develop the risk analysis of a controversial policy.

• "We're too busy. Is not ERM an administrative burden?"
  Integrate ERM methodology into existing processes; e.g., in planning and policy development sessions that need cogent analysis. Test the value of the process by seeing whether it can actually increase efficiency by obviating the need for long unstructured discussions.

• “What if our service plan does not accurately reflect our business?”
Risk analysis can, at a minimum, help identify gaps between professed mission in the service plan and actual work.

- **“We are at the contract negotiation stage in our major project. Can we do a risk analysis?”**
  It is better to build ERM into all stages of the process, starting with project conceptualization. The risk register can eventually be a checklist and guide to final contract arrangements.

- **"What technology do we use to capture risk information?"**
  Initial trials with risk management software showed that simple spreadsheets are more appropriate to support the early proof of concept. Define your processes and information needs first. A mature practice of integrated service planning, performance, and risk management may eventually warrant the use of a specialized application.

- **“Doesn’t ERM challenge traditional government culture and create political risk, especially when risks are subject to Freedom of Information requests?”**
  ERM should challenge traditional culture. We want to move away from unreasoning risk-aversion towards responsible risk-taking.

  Fears of political risk in the sense of sensational criticism, due to the publishing of risks, are not well founded. Comprehensive risk identification and mitigations, documented together, lend credibility to the organization.

  Freedom of Information (FOI) is addressed in the next section.

- **“What do we do once risks are identified?”**
  A completed risk register with mitigations directly informs plans for action, or the design of a contract, a policy or program. It is also a tool for managing risks on a continual basis.

  Over the long term, archived information provides material to detect trends with regard to classification of risks, types of incidents, efficacy of controls, business units incurring risk, etc.

- **“What about opportunities?”**
  Mitigation strategies (treatments), by definition, are opportunities for innovation intended to reduce risk and give better assurance of success.

  Opportunities are inherent in the very program that is being analyzed, and come under consideration in scenario analysis and environmental scans (out of scope in this Guideline). They can also arise unexpectedly in risk analysis as novel ideas. A UK Audit authority remarks: “Failure to take opportunities can be a huge risk in itself... Organizations can miss out on real chances to manage their business better, improve service delivery and achieve better value for money.”
1.3 RISK CULTURE

1.3.1 Introduction: Sensitive Risk information

Government employees can be particularly risk-averse in that they may not wish to record risk information that: 1) contradicts the perceived political will or direction from superiors; 2) could be embarrassing to government if made public; or 3) might lead to legal liability exposure, perhaps in relation to a stakeholder.

Risk Management Branch takes the values of accountability and transparency as a starting point. Core Policy Manual Chapter 14 states: "Each ministry must develop and maintain the culture, processes and accountability structures that facilitate comprehensive risk identification." Particular points enumerated are addressed in following paragraphs.

1.3.2 Risk Information Contradicting Executive Direction

The purpose of generating risk information is to inform decision-making. Recent research on best practices has characterized the positive attitude of executives who understand risk analysis. They say to staff: "1. Tell us the risks, don't hide them; 2. Tell us as early as possible; and 3. Don't try to fix everything yourself". In a progressive culture, management will meet efforts at the staff level with recognition and support – not sanctions.

1.3.3 Risk Information as Potential Political Embarrassment

The responsibility of the civil service toward government is to provide as full an account as possible of the risks that inhere in a proposed course of action – regardless of the decisions ultimately taken. "Organizations that are governed and managed well accept risks knowingly, mitigate risks where appropriate, and endeavour to be prepared for the unknown." (George Morfitt, former Auditor General of British Columbia, A Review of the Fast Ferry Project: Governance and Risk Management).

The very word "risk" has unfortunate alarmist connotations. It is often feared that a statement of risks will be divulged to the public and lead to scandal; moreover, it is unthinkable to some that a government operation might have a few – let alone several or several hundred – risks. They do not understand that risks are very same business issues or contingencies that they have always faced, though perhaps not knowingly or systematically. The reality is that risks of one sort or another will always be there. Therefore (perhaps ironically) the more risks that a government program identifies, analyzes and prepares for, the more secure the program will be.

A simple statement of risks alone can attract criticism. This fact undoubtedly accounts for some reluctance to produce risk registers. However, documentation that includes not only the identification of risk, but its corresponding analysis and plans for treatment (where required) is better able to withstand scrutiny, and lends credibility to the organization. If pro-actively published (through “routine release”), then information requests and sensationalist criticism can be pre-empted.

---

2 Do not confuse: averse = tending to avoid (as in "risk-averse employees"); and adverse = antagonistic, unfavourable (as in "adverse circumstances").
1.3.4 Freedom of Information Requests

Risk management information is subject to the same exceptions to disclosure under the *Freedom of Information and Protection of Privacy Act* treating all other government information. In the event of a request for information under the Act, cabinet confidences, or information harmful to either third party business interests or personal privacy, must be exempted from disclosure. This tends to mitigate the risk of liability.

Under the Division 2 of the FOIPP Act, here are the current exceptions to disclosure:

<table>
<thead>
<tr>
<th>Section</th>
<th>Exception</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Cabinet and local public body confidences</td>
</tr>
<tr>
<td>13</td>
<td>Policy advice or recommendations</td>
</tr>
<tr>
<td>14</td>
<td>Legal advice</td>
</tr>
<tr>
<td>15</td>
<td>Disclosure harmful to law enforcement</td>
</tr>
<tr>
<td>16</td>
<td>Disclosure harmful to intergovernmental relations or negotiations</td>
</tr>
<tr>
<td>17</td>
<td>Disclosure harmful to the financial or economic interests of a public body</td>
</tr>
<tr>
<td>18</td>
<td>Disclosure harmful to the conservation of heritage sites, etc.</td>
</tr>
<tr>
<td>19</td>
<td>Disclosure harmful to individual or public safety</td>
</tr>
<tr>
<td>20</td>
<td>Information that will be published or released within 60 days</td>
</tr>
<tr>
<td>21</td>
<td>Disclosure harmful to business interests of a third party</td>
</tr>
<tr>
<td>22</td>
<td>Disclosure harmful to personal privacy</td>
</tr>
<tr>
<td>22.1</td>
<td>Disclosure of information relating to abortion services</td>
</tr>
</tbody>
</table>

Note that Sections 12, 21, and 22 are *mandatory* exceptions to disclosure (“The head of a public body must refuse to disclose…”); whereas the other sections are *discretionary* (“The head of a public body may refuse to disclose…”).

The difficulty is that it is not always obvious how a given bit of information should be interpreted. For that reason, staff conducting risk analyzes can flag information as *potentially* sensitive, and if in doubt can ask their ministry Director/Manager of Information and Privacy for assistance.

Other potential issues of liability, perhaps in relation to a client or stakeholder towards whom government has contractual responsibilities, can be checked with the help of a legal advisor.

1.3.5 Risk-Aversion versus Risk-Tolerance

One key aspect of the ERM program is to encourage public sector employees to discontinue unnecessarily risk-averse behaviour and to act on new opportunities. Excessive risk-aversion means over-spending on controls; i.e., the uncritical continuation of unnecessary safeguards, bureaucratic processes and non-essential programs. Staff will tend to demonstrate innovation and critical thinking in this regard only when management leads the way by articulating both clear expectations for risk analysis and criteria for acceptable levels of risk.
1.3.6 Recommendations and Resources

Risk Management Branch recommends:

1) political and senior executive leadership to set risk expectations and standards;
2) routine release of non-sensitive risk information, always including mitigation plans; and
3) seeking legal advice regarding liability issues.

Links relevant to risk culture, including public disclosure of risks and mitigation:

British Columbia

- Freedom of Information and Protection of Privacy Act
  http://www.qp.gov.bc.ca/statreg/stat/F/96165_01.htm#section14

- List of Directors/Managers of Information and Privacy:
  http://www.mser.gov.bc.ca/privacyaccess/contacts/DMIP_List.htm

Canada

- Government of Canada: Integrated Risk Management


UK

- UK: Principles of Managing Risk to the Public:

- UK Government: HM Treasury Risk Guidance
  www.hm-treasury.gov.uk/documents/public_spending_and_services/risk/pss_risk_portal.cfm

New Zealand

- Statistics New Zealand: 2005 key risks and risk management strategies:

Australia

- Australia’s Department of Education, Science and Training:
  Annual Report 2004/05: Risk Management
1.4 RESOURCES

1.4.1 Internet Resources

- Those outside government wishing to purchase the AS/NZ standard documents may visit the Standards Australia web site (www.standards.com.au). Government and public sector employees having IDIR accounts, see section 1.4.2 (next).

- Guidelines for Managing Risk in the Western Australia Public Sector, a free download, is a concise guideline based on the AS/NZ standard.


1.4.2 BC Government InTRAnet Resources

- AS/NZS 4360:2004 (standard) and HB 436:2004 (Handbook): See Standards Australia web address in 1.4.1 above. Due to licensing agreements, the standard and companion handbook are available free only to provincial government employees on the following site:

Risk Management Branch ERM Program:

(Click on "Corporate Standards")

1.4.3 Glossary

These two sources are reasonably congruent:

- Appendix 2 “Glossary of Terms” in Guidelines for Managing Risk in the Western Australia Public Sector (see section 1.4.1 above);

- Section 1.3 “Definitions” in AS/NZS 4360:2004. (see section 1.4.2 above).
2 APPLICATION OF ENTERPRISE RISK MANAGEMENT PROCESS

The ERM process is applicable, broadly speaking, to two distinct contexts: 1) the integration of risk management into the organization generally; and 2) a single risk analysis for a strategic plan, service plan, project, program, or policy. “Communicate and consult” and “establish the context” are relevant to both.

2.1 COMMUNICATE AND CONSULT [Refer to Process Diagram page 5]

2.1.1 Consultative Team Approach

“It is important to develop a communication plan for both internal and external stakeholders at the earliest stage of the process. This plan should address issues relating to both the risk itself and the process to manage it” (AS/NZS 4360:2004, p.11)

The consultative team approach means that ERM is not planned artificially, in isolation, and then imposed upon the business from without. Rather, it is developed in concert with those who understand the risks and are best able to identify and manage them.

Communication is often cited as the most commonly ignored aspect of ERM. Ensure not only that risk reporting goes up to higher levels, but also that executive decisions regarding tolerance of risk and priorities for action get communicated back down to the business unit level. This is the only way to build a consistent culture of risk management.

2.1.2 Initial Planning

The following situations show the increase of scope of consultations, depending upon the context. The sponsor organization must determine the correct balance of and limits to direct participation.

a) Scope: executive sponsor; manager and some staff. In planning an introductory ERM exercise, both executive and staff must agree on where risk analysis is most needed and how the session will be evaluated;

b) Scope: broad range of employees with professional expertise. Employees may already be practicing some type of risk management (perhaps informally). These practitioners – they might be social workers; administrative staff; scientists; engineers; etc. – must be involved in the adaptation of ERM to ensure that it answers their business needs;

c) Scope: government, local community, professional and private sector partners. Major projects or complex policy development efforts have several stages and a long time horizon. The sponsor organization enhances its credibility by including stakeholders (e.g., local community interests; financial experts; design and construction experts; legal experts, etc.) in risk analysis.
2.2 ESTABLISH THE CONTEXT [Refer to Process Diagram page 5]

Again, “establishing the context” is described here for two distinct purposes:

1) to inform a Risk Management Plan for the full implementation of ERM in an organization (see section 2.2.1 next); and

2) to prepare for a particular risk identification session (see section 2.2.2).

In either case, “establishing the context defines the basic parameters within which risks must be managed and sets the scope for the rest of the risk management process.” (AS/NZS 4360:2004, p.12)

2.2.1 Context Analysis 1: to Inform a Risk Management Plan

The AS/NZ standard elaborates the notion of context – applied to the organization as a whole – in several aspects; e.g.:

- scan of external and internal environments;
- analysis of stakeholders;
- employees’ perception of risk and development of risk criteria;
- selection of processes or elements of the organization to which risk analysis is applied.

A fully developed analysis of context is appropriate as the organization progresses in its practice of ERM towards a full implementation. It will inform a Risk Management Plan.

A Risk Management Plan (RMP) tells “how risk management is to be conducted throughout the organization” (AS/NZS 4360:2004, section 4.3.1, page 26). It documents the ministry’s or agency’s particular approach to ERM, but in doing so should not duplicate the material in Core Policy Manual Ch 14 and AS/NZ 4360:2004.

The RMP can therefore be brief and concisely set out:

a) policy (expectations of how risk analysis will be integrated with ministry business);

b) accountability structure, (roles/responsibilities, stakeholders, and reporting patterns);

c) resource requirements;

d) plan for information management (see “frequently asked questions” p.10); and

e) scheduled pilot sessions, with provisions for feedback.

It is strongly recommended that the effort to create the RMP is preceded by carrying out risk analysis on a trial basis in order to understand its value and application. The minimum necessary administration and infrastructure should then support the value proposition.

Common reason for program failure: setting up a cumbersome infrastructure with all kinds of formal requirements before the new practice (in this case, risk management) is truly understood and embraced by practitioners.
2.2.2 Context Analysis 2: to Prepare for a Risk Identification Session

A facilitated round-table session is the assumed method here (see section 2.3.1). It is essential for the facilitator/chair carefully to interpret the context and write a brief paper to establish the session’s scope, criteria, and deliverable, using the following 6 headings:

1. **Subject of the risk analysis.** E.g., strategic plan, service plan, project, program, policy, process or procedure. State the scope with respect to organization, hierarchical level, and time frame. Specify whether a strategic or an operational view is being taken.

   Comment: If there is no plan or policy yet created, and a risk profile on a particular issue is needed, then the subject of the risk analysis is the status quo; i.e., the organization’s “current approach” (which may be ad hoc) to the issue. If at least general goals or values can be stated (see next) then the team can generate a risk profile.

2. **Goals and objectives** of the program, policy or plan in question. Risks are best identified in relation to either broad strategic goals (at the highest level of planning) or in relation to objectives and specific activities. The list of goals, objectives and strategies (activities) can serve to structure the discussion of risk.

   Comment: If there is no program of activities designed yet (see previous comment), state highest overall goals, and sketch the main components of a draft plan. This will give a basis to generate a risk profile and mitigations to inform a final plan.

3. **Value criteria.** These are the guiding principles of the organization, such as a professional ethical code, business practices, political priorities, or operating principles. They might be found in existing vision and mission statements. They might take the form of special rules; e.g., how business is to be conducted in a specific context. Participants refer to value criteria in order to help to identify and assess risks.

   Comment: It is important to keep value criteria in plain view during the session. They serve as a common point of reference to help resolve controversy, and formulate and assess risks.

4. **Stakeholder analysis.** The context paper should identify stakeholders, both internal and external, and provide some analysis of their roles, perhaps including an estimation of their degree of influence, interests and motives, and position with respect to value criteria. They can be both bearers and sources of risk. Stakeholder views are represented, directly or indirectly, in a balance determined by the project sponsor.

   Comment: Refer to existing consultation papers. A diverse range of session participants, where appropriate and within the limits of facilitation, lends rigour to the process and leads to a better quality result.

5. **Assumptions and constraints.** Deadlines, time-frames, executive directives or other conditions that somehow limit the risk process itself.

6. **Deliverable for the session:** State the intended product of the session; viz., a comprehensive list of risks, in several categories of analysis, with rankings and summary treatments arrived at by consensus, to inform an improved business plan, policy or program.
2.2.3 Specialized Contexts: Sub-disciplines within Risk Management

Do not let the identification of risk stray out of scope of the defined context. Recognize, too, that certain perils or exposures call for a specialized risk analysis as a separate exercise (see Fig. 4).

For example, non-experts will often bring up the notions of earthquake, hurricane or flood (because that is what the word “risk” connotes to them) in almost any context. Those risks belong to a specialized analysis for emergency and business continuity planning. Similarly, security risks, with respect to physical dangers, facilities, and procedures, requires a security review, which is an expertise unto itself.

These specialized areas bring their own criteria and resources to bear upon the process. Risk Management Branch can assist with many of these specialized sub-disciplines.

Fig. 4. Specialized sub-disciplines within Enterprise Risk Management.

2.3 IDENTIFY RISK [Refer to Process Diagram page 5]

2.3.1 Risk Identification Methods

[See section 2.8.2 for Risk Register template to begin recording risk statements.]

Risk identification:

“...requires the ability to visualize how particular sets of circumstances might cause both routine and extraordinary accidental losses. [...]”

Exposure identification and analysis are at least as much an art as a science, relying both on insight and imagination. A number of basic methods have been developed to search for loss exposures.” (Head., G., Horn, S., Essentials of Risk Management, 3rd ed., 1997 - p.3.4 and p. 3.39)
The “basic methods” provide a way to impose some order on an otherwise unstructured search for risks. These include surveys, loss histories, flowcharts, and “expertise within and beyond the organization.” The Guidelines for Managing Risk in the Western Australia Public Sector (see section 1.4.1) list includes the following:

- interview/focus group discussion
- audits or physical inspections
- brainstorming
- questionnaire, Delphi technique
- networking with peers, industry groups and professional associations
- judgemental – speculative, conjectural, intuitive
- history, failure analysis
- examination of personal experience or past agency experience
- incident, accident and injury investigation
- scenario analysis
- decision trees
- strengths, weaknesses, opportunities, threats (SWOT) analysis
- flow charting, system design review, systems analysis,
- work breakdown structure analysis

The AS/NZ standard lists similar techniques; they must be selected according to “the nature of the activities under review, types of risk, the organizational context and the purpose of the risk management study” (AS/NZS 4360:2004, p.16).

All of the above is really an admixture of information gathering techniques, discussion formats and specific types of content. This Guideline focuses on the following method:

1. TECHNIQUE
**Facilitated round-table sessions** with subject-matter experts, in-house experts and outside stakeholders or representatives, as appropriate. A 6-8 person group is ideal. If an in-house person can effectively chair a meeting, that person should be able to lead the risk process. (An outside facilitator may be needed at first.) A scribe can assist.

2. DISCUSSION FORMAT
**Review of the goals, objectives and strategies (activities), and value criteria** set out in the context paper. **Performance targets** also give a good structure. Risks are identified methodically in relation to the goals, objectives, strategies, and values. The question is: “What risks threaten the accomplishment of this particular goal/task/performance target?” Or: “What risks threaten the preservation of this core value?”

3) CONTENT
**Professional memory of participants, as well as a list of generic risk categories** for review, are relied upon to help ensure that the analysis contemplates all types of risk. The question for participants is: “What are the risks in this category [e.g., financial; legal; technical; HR] that threaten the accomplishment of this goal/objective/program activity?”

The Western Australia document lists “sources of risk”, while Risk Management Branch has developed the Risk Dictionary (see ERM InTRAnet site under Tools and Resources) of risk categories suitable for the analysis of public sector programs.
2.3.2 How to State Risks

There is an art to discerning what constitutes a risk, and to expressing it in such a way that it can be effectively managed.

a) Specify the distinct risk that hinders a specific objective. State cause + effect, with a joining word such as “causes”, “leads to”, “prevents”, “hinders”, etc. Do not state general unfavourable conditions, in and of themselves, as risks.

**Examples**

Poor risk statements:
- Budget cuts.
- Cumbersome bureaucratic processes.

Better risk statements:
- Possible 10% budget cut prevents accomplishing deliverable x.
- Complex approval process prevents accomplishing time-sensitive deliverable y.

b) Select a defined moment in the chain of events that is within the organization’s control. Do not state more than one risk at a time.

**Example**

Poor risk statement:
- Accidental event xyz happens causing environmental damage, health hazard and possible litigation which leads to loss of reputation and political risk.

Better risk statement:
- Failure to ensure effective environmental controls leads to accidental event xyz.

c) Recognize risks that originate beyond the control of the organization, but that have a specific impact and therefore require contingency planning.

**Examples** (in the context of a new design for workflow within an electronic payment service):

Poor risk statement:
- There might be a power outage. It will affect everything, and Ministry will be unable to process payments. [Note: rejected as beyond agency’s control and out-of-scope.]

Better risk statement and recognition of the specific impact:
- Natural or other disaster causes power outage and prevents workflows for mission-critical payment systems. [Note: Treatments to be developed in a Business Continuity Plan.]

Poor risk statement:
- Ministry delays all investments and wipes out our program. [Considered beyond control.]

Better risk statement and recognition of specific impact:
- Ministry delays all IT investments, preventing implementation of servers for e-payments. [Note: Treatments can include: 1. review manual systems; 2. improve engagement and advocacy with Ministry IT planning group.]

d) Use caution in presenting risk registers that are pre-populated with generic risks. They may be inaccurate; they may not be properly formulated to be manageable; and participants may not own them. Such lists often stifle the brainstorming process.
2.4 ANALYZE RISK [Refer to Process Diagram page 5]

2.4.1 Risk Analysis Matrix: Likelihood, Consequence, Ranking

Risk analysis signifies establishing levels of Likelihood (probability that the risk will actually occur) and Consequence (the degree of severity of the effect). The resultant calculation is the Ranking. Notice the descriptors for each of the 5 levels are generic – they apply to any program content. Both operational and strategic views are given.

**LIKELIHOOD** = Probability of the risk event actually occurring.

<table>
<thead>
<tr>
<th>Score:</th>
<th>Descriptor:</th>
<th>Approximate probabilities:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Improbable; Rare</td>
<td>0.00 - 0.04</td>
</tr>
<tr>
<td>2</td>
<td>Unlikely</td>
<td>0.05 - 0.24</td>
</tr>
<tr>
<td>3</td>
<td>Possible</td>
<td>0.25 - 0.54</td>
</tr>
<tr>
<td>4</td>
<td>Likely</td>
<td>0.55 - 0.89</td>
</tr>
<tr>
<td>5</td>
<td>Certain</td>
<td>0.90 - 1.00</td>
</tr>
</tbody>
</table>

**CONSEQUENCE** = Degree of severity, with respect to goals/values, should the risk event occur.

<table>
<thead>
<tr>
<th>Score:</th>
<th>Descriptor:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Insignificant</td>
</tr>
<tr>
<td>2</td>
<td>Minor</td>
</tr>
<tr>
<td>3</td>
<td>Significant</td>
</tr>
<tr>
<td>4</td>
<td>Major</td>
</tr>
<tr>
<td>5</td>
<td>Catastrophic</td>
</tr>
</tbody>
</table>

**RANKING L x C Matrix**

<table>
<thead>
<tr>
<th>Score</th>
<th>LOW</th>
<th>MEDIUM</th>
<th>HIGH</th>
<th>EXTREME</th>
<th>EXTREME</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

LIKELIHOOD 1 2 3 4 5

CONSEQUENCE
2.4.2 Inherent vs. Residual Risk

Risks are assigned L and C by considering them in the absence of existing controls – that is, it is the inherent risk that is ranked. This departs from the advice in the standard (see AS/NZS 4360:2004, section 3.4.3, p.17). The rationale for considering inherent risk is to be able to consider separately the relative cost and effect of controls, and identify, for example, over-spending to control insignificant risks.

Ranking residual risk (i.e., the level of risk after controls) is usually too complicated and unnecessary, except when working out detailed risk financing solutions.

2.4.3 Advice on Assigning Likelihood & Consequence

Likelihood is the probability that the risk event identified will actually occur. It is, in most cases, the likelihood of the causal event with which we are concerned (while the effect connected with it is taken as a certainty)\(^3\).

If statistical data exists to support distribution probabilities with respect to Likelihood and severity of the impact of the risk, it can be brought to bear on the analysis.

However, ministries must often estimate Likelihood without the benefit of quantified historical data. They must rely on professional memory and qualitative information to select “Unlikely”, “Likely”, “Certain” etc. – and then assign a numerical ranking. Note that the “Approximate probabilities” are not to be taken literally; they are just a convenience for those who prefer to estimate in terms of numbers. While each ranking may not have scientific accuracy, it should at least reflect the experts’ opinion of the risk’s relative importance.

The AS/NZ standard offers the following caution with regard to semi-qualitative analysis (i.e., the practice of assigning a numerical scale to qualitative descriptors):

“Care must be taken with the use of semi-quantitative analysis because the numbers chosen may not properly reflect relativities and this can lead to inconsistent, anomalous or inappropriate outcomes.” (AS/NZS 4360:2004, section 3.4.4, p.18).

The use of “Frequency” in lieu of Likelihood is not recommended. A risk event might have very low frequency (e.g. “once in a career”), but if evidence shows the event is imminent, the Likelihood may be “Certain”. Specify the time-frame in the context.

Consequence is the degree of severity of effect upon goals, objectives, or values, should the risk occur. The descriptors for Consequence (Risk Criteria) given on p.22 are applicable in diverse contexts. However, a ministry or public sector entity can invent the Risk Criteria appropriate to their lines of business (perhaps quantifiable in terms of budget dollars). Many organizations develop a “scorecard” with several categories of consequence. See AS/NZS 4360:2004, s. 3.2.5, p.15.

---

\(^3\) In a review of several ministries’ risk registers, Likelihood referred to the probability of the causal event in 80% of cases.
2.5 EVALUATE RISK  [Refer to Process Diagram page 5]

2.5.1 Risk Evaluation Means a Finer Assessment

Use judgement in deciding whether to enter into risk evaluation when you are just becoming familiar with the process. Many organizations find that to *identify, formulate, and rank risks according to consistent criteria* is enough to proceed to treatment or mitigation (section 2.6). Risk evaluation provides a finer assessment – more checks and balances on risk decisions.

2.5.2 Existing Controls; Tolerance; Action

Risk evaluation consists in considering the ranked risk in relation to: 1) existing controls and 2) the organization’s tolerance for the particular risk in question. The purpose is to arrive at a decision as to how to respond to risks – not as unthinking reaction, but as dictated by specific value criteria and cost/benefit. Each of the following can be entered into the risk register columns (see sample risk register section 2.8.2).

1. *Characterize, in qualitative terms, the existing controls* (i.e., How would you describe the process, policy, device, practice or other action already in place that mitigates the risk in question?):
   - Non-existent; Weak; Adequate; Robust; Excessive (this latter indicates over-controlling and so possibly overspending)

2. *Characterize the risk in relation to the organization’s degree of tolerance*:
   - Unacceptable; Acceptable with treatment; Acceptable

   It is possible to have ‘zero’ tolerance for certain risks (assuming one can avoid them). A risk may be “Acceptable” either because it is inevitable and too prohibitive to treat, or because it is inconsequential and not worthwhile to treat.

   Note: ministries may develop over time fully developed risk criteria or, for example, quantified scales of risk tolerance or risk thresholds. See discussions of criteria, tolerance and threshold in NH 436 2004 (Handbook).

3. *Decide on consequent action*, based on steps 1) and 2):
   - Avoid; Treat; Monitor only (tolerate)

   A risk, if unacceptable, might be avoided altogether by not doing the action that would incur it in the first place. If it is not possible to avoid the risk, and treatment is impracticable or prohibitive, then it can only be tolerated and monitored. Risks that are inconsequential, but whose status might change, can be monitored.
2.6 **TREAT RISK** [Refer to Process Diagram page 5]

2.6.1 **Diversity of Risk Treatment (Mitigation)**

As indicated in section 1.1.1, treatments (risk mitigation) can consist of virtually any sort of administrative action, as well as the application of specialized disciplines – where a separate analysis may be required; e.g., emergency planning, business continuity planning, security planning, risk financing; financial controls; human resources management. Grouping risks in categories can help in the design of cost-effective treatments.

2.6.2 **Ensuring Effective Risk Treatment (Mitigation): Advice for Facilitator**

In government and public sector work, three points are necessary to underscore:

1. *Treatments are, by definition, new measures undertaken to mitigate identified risk.* At times, participants fall into familiar thought patterns and merely repeat the list of existing controls, and say there is nothing more to be done. Or, they may say that the implementation of their planned program activities constitutes mitigation of risk. It is just here where the facilitator or risk champion may add value:

   - A facilitator can lead off by asking (either naive or well-informed) questions about possible treatments and stimulate discussion;

   - A facilitator can draw attention to the ranking of the risk – if participants are reminded that it is high or extreme, and threatens the viability of the program, they will feel less inclined to leave the matter unattended;

   - A facilitator can introduce categories of implementation risk (well-documented common reasons for program failure) to inform the analysis;

   - The necessity to study the issue and develop treatments “off-line” or in a separate session can be flagged;

   - The possibility of inviting expertise from outside the immediate group can be raised;

   - At a minimum, the action of documenting the risk and bringing it to the attention of a higher authority or other entity constitutes an improvement in the management of the risk.

2. *Treatments must be documented.* During the latter part of a risk identification and analysis session, make summary statements of treatments. They might have to be elaborated (see next), but briefly summarizing them allows the facilitator to cover a maximum amount of material. A measure of due diligence is achieved by recording both the risks and how they will be managed.
3. *Treatments must be translated into action.* Suggested treatments (mitigation of either a risk likelihood or degree of consequence) are subject to cost-benefit analysis. The facilitator must challenge the participants to commit to acting upon mitigation strategies. If the ERM initiative is meant to enhance existing processes, then the treatments must become new items in the list of project tasks or business plan strategies.

2.7 **MONITOR AND REVIEW** [Refer to Process Diagram page 5]

2.7.1 **Monitor: Regular Management of Risk Information**

Monitoring has to do with managing your risk information as a regular practice.

Risks themselves undergo change, and can require revision in terms of their description and ranking. New risks appear. Old material requires scoring through (but not deleting) and archiving. Therefore, a periodic updating of risk information, using the risk register as a management tool – perhaps the first agenda item in regular meetings – is recommended.

Repeat note on software: Initial trials with risk management software showed that simple spreadsheets are more appropriate to support the early proof of concept. Define your processes and information needs. A mature practice of integrated service planning, performance, and risk management may eventually warrant the use of a specialized application. Plan the consistent management of risk information going forward.

2.7.2 **Review: Historical Risk Information**

In a mature practice of risk management, a body of information is developed over time to develop analyzes of: the risks themselves; their most common sources (categories of risk); their levels of actual occurrence; the efficacy of treatments; and the occurrence of unforeseen events. All of this serves to better manage risks and inform planning. See, e.g., HB 436: 2004 section 9.5.

2.8 **RECORD THE RISK MANAGEMENT PROCESS**

2.8.1 **Summary: Documentation of ERM**

Documentation of ERM has so far been discussed with regard to:

1. a fully developed Risk Management Plan for organization-wide implementation – see section 2.2.1;

2. a brief context analysis to prepare for a particular risk identification session – see section 2.2.2;

3. the documentation of treatment strategies by their inclusion in existing project and service plans – see section 2.6.2;

4. the development of historical risk analysis (in a mature practice of ERM) – see section 2.7.2.
2.8.2 Risk Register

The standard Risk Register shown here can be modified to suit the organization’s needs; e.g., project management functions such as person accountable, deadline, budget impact, etc., can be added.

Excel spreadsheet template available to government employees:
Risk Management Branch ERM Program:
(Click on “Tools and Resources” and “Sample Risk Register”)

Fig. 5 Risk Register Standard Template

<table>
<thead>
<tr>
<th>Description of Risk</th>
<th>L</th>
<th>C</th>
<th>Inherent Risk Rating</th>
<th>Risk Category</th>
<th>Existing Controls; non-assistive weaken assistive: robust moderate precaution</th>
<th>Risk Tolerance =&gt; Action: monitor only; treat avoided</th>
<th>Mitigation Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Item 1</td>
<td>1</td>
<td>1</td>
<td>LOW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Item 2</td>
<td>1</td>
<td>5</td>
<td>HIGH</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Item 3</td>
<td>2</td>
<td>3</td>
<td>MEDIUM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Item 4</td>
<td>2</td>
<td>5</td>
<td>MEDIUM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Item 5</td>
<td>3</td>
<td>4</td>
<td>HIGH</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Item 6</td>
<td>4</td>
<td>4</td>
<td>MEDIUM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Item 7</td>
<td>4</td>
<td>5</td>
<td>EXTREME</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Item 8</td>
<td>5</td>
<td>5</td>
<td>EXTREME</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

EXPLANATION OF COLUMNS IN SAMPLE RISK REGISTER:

Context Descriptor [not shown]
User-defined field to organize risks by program, project, business unit, etc.

Risk Description [essential]
Description (): state a discrete risk in one concise statement – see section 2.3.2.

L., C., Inherent Risk [essential]:
Likelihood, Consequence and Inherent Risk Rating (automatically calculated) – see section 2.4.1.

Risk Category
Assigning category of risk to each line entry can help later to design treatments and analyze sources of risks – see section 2.3.1.

Existing Controls; Risk Tolerance and Consequent Action
See section 2.5

Mitigation Strategy [where treatment is required, statement of treatment is essential]
See section 2.6