At Risk

Volume 18, Issue 2 **Fall/Winter 2010**

A Risk Management Newsletter for the British Columbia Provincial Government, its Ministries and Organizations

In this Issue:

Please feel free to copy and distribute this edition of At Risk.

To receive future electronic editions of At Risk please e-mail RMB@gov.bc.ca with "At Risk" in the subject line and include your e-mail address.

Executive Director's Message

Modern risk management originated with risk financing schemes set up by clever and enterprising Romans over 2000 years ago. Earlier examples of robbery and life insurance appear around 2000 years before that. The practice evolved from selling insurance-type products, to alternative forms of managing risk, to the multi-disciplined spectrum of functions we see today. Many specializations have emerged, for example: security, business continuity, occupational health and safety, legislation (e.g. no hand-held devices while driving), and loss prevention.

For each, the basic principles are the same: consideration of the likelihood and possible consequences of an event, and then taking measures to minimize the chance of the event occurring or the damage it inflicts if it does occur. "An ounce of prevention is worth a pound of cure." (Benjamin Franklin)

Far from being the flavour of the month, risk management has been around in some form for over 4000 years. Its application and tools continue to evolve, as this issue of *At Risk* illustrates.

Staff at Risk Management Branch are always available to provide assistance on whatever risk management means to you and we welcome your enquiries.

Phil Grewar, Executive Director

The New Risk Register

From time to time we come across innovations in our community that make so much sense we wonder how we made do without them. That was the case when a Ministry of Health Services risk manager showed us their risk register.

Their innovation was to split up the risk identification into three components: Event, Causes, and Impacts. We wrote about this new way of defining the risk statement in an earlier *At Risk* http://www.fin.gov.bc.ca/pt/rmb/ref/AtRiskFallWinter2009.pdf and refined it during the recent Pandemic and Winter Olympic ERM projects. It is now the basis for the new and improved *Standard Risk Register Template*.

In addition to adopting this three-part risk identification method, Risk Management Branch has made further changes to the template to facilitate risk communication, consultation, reporting and review – each important parts of the risk management process. This was done through the addition of several new columns.

Expanded Risk Management Strategies

The best risk register is of no value if its proposed mitigation strategies are not acted upon. The new "Risk Management Strategies" columns allow the risk register to be used as a practical work plan by clearly defining:

Deliverable: What form will this mitigation take? Will it be a formal project plan, a detailed report, Treasury Board submission, or Cabinet submission? This column defines exactly what the product of the mitigation strategy will look like.

Required Resources: What is needed to develop and implement the mitigation? This column could be where you articulate required authorizations, budget, time, or staff to put the mitigation plan into action.

Task Owner: Who has been assigned responsibility for this mitigation? Identify someone by name to ensure accountability in this column; and

(Continued on page 2)

The New Risk Register (continued)

DELIVERABLE (what form will this mitigation take? A formal plan, a report, TB or Cab Sub ... Etc.)	REQUIRED RESOURCES (What is needed to develop and implement the mitigation?)	TASK OWNER (Who has been assigned responsibility for this mitigation?)	DUE DATE (When is the deliverable to be ready?)

(Continued from page 1)

Due Date: When is the deliverable due? Without a firm due date, tasks sometimes get set aside.

Three Additional Risk Ratings:

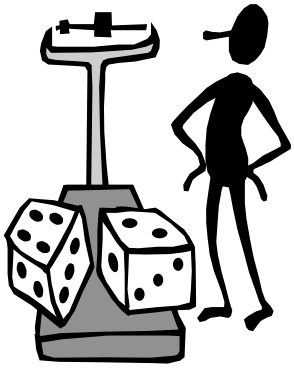
Target Risk Rating: This is the risk rating expected or predicted once all proposed mitigations are in place. This is an important step as it allows executive to see whether the proposed mitigations are likely to achieve a result that is satisfactory, if the expected risk reduction is worth the required resources, or if even more resources should be committed to lower the risk further.

Risk Tolerance Rating: This is the maximum level of risk executive is willing to accept for this event. This should be provided by executive after having been briefed on the risk, existing and planned mitigations, and associated costs. It is closely related to Target Risk Rating; when Target Risk and Risk Tolerance ratings are congruent, we know that the risk mitigation strategy should lower risk to a level our executive is comfortable with.

Current Risk Rating: When risk management is applied to a project on an ongoing basis with regular feedback and updating on risk mitigation implementation, the periodic rating of current risk allows executive to see the progress made to date. Ideally, Current Risk Rating approaches Target Risk over time. If not, this can serve as an important flag that a change of strategy and/or more resources are required.

Tracking and Reporting Columns

Four additional "Tracking" columns allow risk managers to identify progress to date, any issues or comments about why things are progressing well or stalled, further action that's required, and a completion date when the risk is expected to be managed to within executive's risk tolerance.



Any of these additional columns can be hidden from the register if not required. Particularly if just introducing the risk management process to a working group, you may wish to hide those columns until needed so as not to intimidate those around the table with an arm-long document.

Check out the new *Standard Risk Register* with its expandable new columns, and feel free to customize it to meet the specific needs of your organization. You can find it on the Risk Management Branch Intranet site http://gww.fin.gov.bc.ca/pt/rmb/erm/ermTools.stm , or contact Risk Management Branch RMB@gov.bc.ca and we'll be happy to email you a copy.

TARGET RISK RATING *(Risk rating expected / predicted once all mitigations are in place.)*				CURRENT RISK RATING *(Current level of risk in light of mitigations implemented at this report period.)*				RISK TOLERANCE RATING *(Maximum level of risk executive is willing to accept. This should be provided by executive after having been briefed on the risk, existing and planned mitigations, and associated costs)*			
LIKELIHOOD (1-5)	CONSEQUENCE (1-5)	TOTAL SCORE 1-25)	RISK RATING	LIKELIHOOD (1-5)	CONSEQUENCE (1-5)	TOTAL SCORE (1-25)	RISK RATING	LIKELIHOOD (1-5)	CONSEQUENCE (1-5)	TOTAL SCORE (1-25)	RISK RATING

Multi-Function Device Information Risks

In today's office environment the photocopier is ubiquitous but it isn't just a photocopier anymore. Many photocopiers are now referred to as Multi-function Devices (MFD) and have a number of input sources. These can include the internet or a Local Area Network (LAN), and a phone line allowing them to be used as printers, scanners and fax machines as well. It's a useful office tool that can also pose significant risks to our organization and it is important that we recognize those risks and take steps to limit them.

Possibly the most widely recognized risk is that the document you have just copied, scanned or faxed will be left in the machine and someone else will come by and pick it up, compromising that document's information. Some, but not all, of the newer machines have an alarm installed to warn you when you forget the original, however if you are in a rush you may be well away from the machine before it starts beeping at you. Always ensure you retrieve your original documents as soon as you are done.

Consider the MFD's scanning function. Once the document has been scanned and resides in the machine's memory it has to be sent somewhere, usually to an email address that you type in. If you enter the wrong address, you cannot assume that the document is just gone. Take special care to enter the correct address to ensure your document isn't sent to the wrong mailbox.

One recently discovered vulnerability for scanners is that some makes and models can be remotely activated over the LAN or the internet (depending on your network configuration). By default, the machines are set up to use this remote access function, but it can also be activated through a web browser. Using simple command scripts vulnerable scanners can be operated remotely and information left behind on the scanner bed is at risk. Deactivate this remote access feature if your machine has this ability.

Today's machines use a hard drive to store the image being reproduced. Depending on the settings and the size of the hard drive the image may outlast the life of the copier. As a result, there is potential for the next owner to steal identities or otherwise profit from information on the hard drive.

There are a variety of methods to reduce the risk of data stored on the hard drive. The first is to purchase a machine that deletes the data after it has completed the print or scan job. The next option is to have the hard drive wiped when the machine is being taken out of the office. Finally, you can have the hard drive removed and then physically destroy it to protect your data. This may be your best option to protect the information that has been stored on the hard drive.

Even basic printers have built-in memory that stores print jobs. If the printer runs out of paper the print job will reside in memory until more paper is added. This is convenient if one is aware that they have not printed the entire document. There is more risk if there are only a few pages missing from the end and the user doesn't realize they are missing. When more paper is added the final pages print out, putting your information at risk. Verify your documents each time you retrieve them from any printer.

If your office is using a centralized printer and you neglect to retrieve a document right away, it will be available for anyone else walking by. This problem is exacerbated by having numerous printers attached to your LAN that you can choose to use. Ensure you print to the right location to avoid making your document available to strangers.

A growing risk in today's copyright-aware society is that an employee will make an illegal copy on your machine and your organization will be liable for the employee's actions. It is important for everybody to know what can and cannot be copied. Your organization's copying policy should be posted prominently near your MFD.

Although today's MFD technology creates a number of information-related risks, these can be mitigated relatively easily and with minimal cost. Like so many risk areas in this day and age, education and awareness of the risks, and simple reminders about the easy mitigations, go a long way to reducing the likelihood that a loss will occur.

Ask Risk

What is the difference between the role of the "Government Security Office" and other security functions across government?

Great question! Best to begin our answer by establishing a common understanding of "security" using the definition found in the Core Policy and Procedure Manual Glossary: *"Security – Risk control techniques to protect people, assets and the operations of government from loss or harm."*

The Government Security Office acts to ensure that the various security elements across government function in a coordinated way to achieve the highest levels of protection for our people and our assets. In the context of security, the maxim about the weakest link in the chain holds true. For example, we have very robust network security but sensitive information could still be exposed through social engineering, careless handling of documents, work-related conversations within earshot of unauthorized listeners, etc.

In the same way that Air Traffic Control coordinates aircraft movements to assist safe efficient operations, or an operating system manages files, memory and storage for a computer, the Government Security Office works to harmonize the various security elements to extract the greatest benefit for government. It makes sense that security policies and resources be coordinated to avoid duplication or conflict.

Formally, the mandate for Government Security is ascribed by policy to the Executive Director of the Risk Management Branch, and the Government Security Office resides therefore within Risk Management Branch.

The Executive Director, Risk Management Branch, is the government's senior security officer responsible for:

- overall planning, direction, monitoring and evaluation of government security management;
- developing, maintaining and co-ordinating the government security policy, operational standards;
- guidelines and procedures; and
- providing advice and assistance on security.

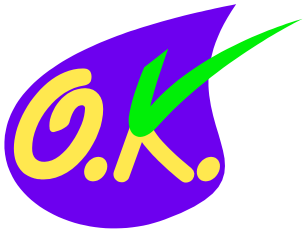
Every public servant and each Ministry has a responsibility for security but particular roles and mandates are recognized within four primary areas: personnel, information, information technology, and physical assets. Thus the Government Security Office works with the B.C. Public Service Agency [personnel], the Office of the Chief Information Officer [information and information technology] and with Shared Services B.C. Accommodation and Real Estate Services [physical assets]. A breach of security in any one of those areas can negatively impact the others so it is critical that they are harmonized and interlocking in their policies and programs.

The Government Security Office chairs the Government Security Advisory Committee which is made up of the Ministry Security Officers. Part of the 'big picture' available to the Government Security Office comes from that kind of liaison and input but also from receiving and reviewing all General Incident or Loss Reports (GILRs) for government. Learn more about GILRs at http://www.fin.gov.bc.ca/ocg/fmb/manuals/FAP/FAP_L.htm#m1

Government Security Office staff hold Canadian Risk Management designations, ASIS International Board Certifications in both Security Management and Investigations, and are appointed as Special Provincial Constables. They have previously served in law enforcement or military and have experience and training in security, loss prevention, threat assessment, intelligence analysis, investigations, counter terrorism and close protection. They can be reached at RMB@gov.bc.ca or 250-356-1794.

Risk Management in Contracts

Contracting is a key tool for obtaining services, delivering programs, and for transferring risk. Risk Management Branch (RMB) reviews a lot of government contracts, often in the context of advising about indemnity and insurance. However, the scope of our review is much broader than that, and yet it's not a legal review. We don't provide legal advice, nor are we a substitute for your seeking legal advice or procurement expertise.



You can conduct your own risk management review of any contract using this sample checklist as a guide:

- ☐ The contract is consistent with the terms of the procurement process. Depending how the procurement document was written, some contract clauses will be non-negotiable and should not be changed.
- ☐ Parties to the contract are legal entities and the correct legal names (or defined terms) are used throughout the contract.
- ☐ All defined terms and definitions used consistently throughout the agreement.
- ☐ The services to be performed are described in detail.
- ☐ Performance measures and reporting requirements are set out clearly.
- ☐ Any changes to the contract are required to be made in writing and signed by all parties.
- ☐ British Columbia is the jurisdiction for law.
- ☐ Assignment of the contract to another party is not allowed without written approval of the Province.

- ☐ Subcontractors must be approved by the Province and bound by all the same terms and conditions as the primary contractor.
- ☐ Privacy and confidentiality issues are addressed and contractor is obligated to follow *Freedom of Information and Protection of Privacy Act*, if applicable.
- ☐ Termination provisions are specified and reasonable.
- ☐ Dispute resolution processes are specified and formal dispute resolution (arbitration and mediation) is based in British Columbia.
- ☐ Appendices and/or schedules referred to in the contract are attached, and there is a clear order of precedence in the event of conflicting terms.
- ☐ Insurance requirements are specified, they relate to the risk of the services being performed, and standard approved language has been used so that the contractor and their insurers are able to comply with the requirements.
- ☐ The Province's boilerplate indemnity provision is intact — the contractor is indemnifying the Province. No modifications to this boilerplate language are permitted without prior approval of RMB.
- ☐ If there are limitations of liability, they are reasonable given the context of the contract. The Province will not limit liability on certain types of loss — if in doubt discuss with RMB.
- ☐ Any proposed indemnity from the Province to the contractor is reasonable and has received formal approval from RMB. For more on approval of indemnities granted by the Province see: http://gww.fin.gov.bc.ca/PT/rmb/forms/indemnityapproval.stm

Ongoing Risk Management Education

- **British Columbia Risk & Insurance Management Association (BCRIMA)**
  BCRIMA provides education primarily through monthly luncheon speakers and a spring Professional Development Day session. Educational opportunities are posted on the BCRIMA website as they become available:
  http://britishcolumbia.rims.org/RIMS/BritishColumbiaChapter/Home/

- **Canadian Risk Management (CRM) Program**
  Simon Fraser University offers evening courses toward the CRM designation in downtown Vancouver and downtown Victoria. For more information call them at 778-782-5095, see http://www.sfu.ca/cstudies/mpprog/rims.htm, or send an email to mpp-info@sfu.ca

  University of Northern British Columbia offers weekend courses toward the CRM designation in Prince George. For more information call them at 1-866-843-8061, see http://www.unbc.ca/continuingstudies/certificates/riskmanagement.html or send an email to cstudies@unbc.ca

Risk Management Conferences

- **RIMS 2011 Annual Conference** May 1-5, Vancouver, British Columbia
  http://www.rims.org/annualconference/RIMS2011/Pages/default.aspx

- **2011 RIMS Canada Conference** September 18-21, Ottawa, Ontario
  http://conference.rimscanada.ca

- **2011 Western Regional RIMS Conference** Las Vegas, Nevada
  http://nevada.rims.org/RIMS/NevadaChapter/2011WRCNV/Default.aspx

Risk Management Resources

- Risk Management Magazine http://www.rmmagazine.com/

About Our Organization . . .

Risk Management Branch and Government Security Office staff just received two Ministry of Finance's APEX awards. Glen Frederick, Director of Client Services for Core Government and Crowns, was part of the project team that won the Innovation award for the creation of an alternative and more cost effective public-private partnership financial model. Our Executive Director Phil Grewar received a Leadership award for promoting risk management in government and realizing a conservative net savings to government of $1 billion through our innovative self-insurance programs. Four other staff were also nominated in the Performance Excellence category for the Enterprise Risk Management program.

To learn more about Risk Management Branch and Government Security Office visit our internet site: http://www.fin.gov.bc.ca/PT/rmb/index.shtml or give us a call. Government staff may access our Intranet: http://gww.fin.gov.bc.ca/PT/rmb/index.stm

It should be clearly understood that this document and the information contained within is not legal advice and is provided for guidance from a risk management perspective only. It is not intended as a comprehensive or exhaustive review of the law and readers are advised to seek independent legal advice where appropriate.

At Risk

is published
twice yearly by the
Risk Management Branch
and Government Security
Office
Ministry of Finance
Province of British Columbia

MAILING ADDRESS:
PO Box 3586
Victoria BC V8W 1N5

PHONE:
(250) 356-1794

FAX:
(250) 356-6222

CLAIMS FAX:
(250) 356-0661

E-MAIL:
RMB@gov.bc.ca

To view previous editions of ***At Risk*** please visit our Internet site:
http://www.fin.gov.bc.ca/PT/rmb/AtRisk.shtml

Comments, questions, requests for further information about the contents of this newsletter, or questions for possible inclusion in our ASK RISK column, can be directed to "At Risk Editor" via email at RMB@gov.bc.ca or faxed to (250) 356-6222.