AT RISK

Please feel free to copy and distribute as necessary. If you would like to receive an electronic version of this publication just drop us a line at RMB@gov.bc.ca and we will add you to our distribution list.

Executive Director's Message

Welcome to the Spring/Summer 2006 Edition of At Risk, the first publication using our new format.

In this edition you can find updated ERM implementation information; read about water damage and the importance of a timely and effective response; get tips on minimizing the impact of pandemic flu on your organization; and find out how security works for you.

In future editions we will be describing our the new team structure within the branch, introducing our client services teams, and identifying how these changes will help us continue to deliver quality service to our clients.

We hope you enjoy the publication and find it both useful and informative.

Please feel free to contact us with any suggestions for future topics at RMB@gov.bc.ca and, as always, we will do our best to accommodate you.

Enterprise Risk Management (ERM) Implementation

In this third article in a series[1] dedicated to ERM we will review the question of implementation. Advice on the implementation of an ERM program is given in the *ERM Guideline ver*2.1[2]; this includes examples from the BC provincial public sector, "getting started", and a discussion of several aspects of risk culture (e.g. the handling of sensitive risk information, freedom of information requests, and risk aversion). In the present article, the lessons learned from extensive study of what makes implementation successful – in any sort of program or management initiative – are applied to ERM.

Two models
One widely-accepted model of implementation by Mazmanian and Sabatier[3] distils the many variables affecting program success into "six conditions of effective implementation", which apply in both "top-down" and "bottom-up" implementation styles. First, program objectives need to be clear and consistent. Then, the program must incorporate adequate causal theory – that is, it must correctly identify and address root problems in order to achieve desired outcomes. There must be structured support for the achievement of objectives, that is, an integrated system, properly resourced, to achieve deliverables. The commitment and adequate management skill on the part of those implementing is crucial, as is the support of stakeholders who are the beneficiaries of the program. Finally, there must be relative stability in external conditions and management priorities.

Enterprise Risk Management (ERM) Implementation (cont)

In another cornerstone piece in implementation literature, *Up and Running – Integrating Information Technology and the Organization* (Harvard Business School Press, October 1989) by Richard Walton, similar prescriptive principles are explained. Although Walton's subject is IT, his model is relevant and in fact coincides with Sabatier's points. He further recommends that a program receive phased, or staged implementation, with mechanisms to ensure user input, feedback and continuous improvement.

Summary list
The implementation principles given thus far can be summarized as follows:

1. Clear goals and objectives;
2. Adequacy of the program to address problems identified;
3. Practical tools and guidelines – supported through resources – to achieve deliverables;
4. Political, senior executive and management support;
5. Staff and program beneficiary support;
6. Stability in the policy and implementation environment;
7. Phased implementation, with provisions for feedback and improvement.

Many of these points, such as "management support", will seem obvious to public sector managers. The whole question, though, is how the business at hand is interpreted, and how the principles are applied, in order to ensure that risk management techniques are adding value and meet with success. It is worthwhile elaborating a bit on, for example, the second point in the list to illustrate this.

Program adequacy
Does your application of ERM meet the test of "program adequacy"? That is, does the program (in this case, the application of risk analysis) actually address the problems that were identified at the outset? From one aspect, this is a simple question, since ERM is already a developed and proven method to address the problem of identifying risk.

But, assuming that the reason for doing risk analysis is significantly deeper than mere compliance, we can consider how adequate a methodology ERM actually is in different contexts. For example, in strategic planning, if there is difficulty in determining priorities to set direction and allocate resources, a risk analysis facilitates these decisions and makes them defensible. On the operational side, if there is concern that the business plan is impractical, collects dust, and does not really reflect the organization's activity on the ground, then risk methodology will definitely discover that misalignment. If, to take another scenario, a given program or administrative practice consists of a confused history of various policies, methods and outcomes – while a coherent and transparent program is actually sought – then a risk analysis will inform the new design.

In all cases, it is a question of accurately establishing the context, and making explicit the value criteria by which risks are identified and ranked. This is partly why ERM is a robust methodology that is adequate to the task at hand.

In reviewing the conditions for successful program implementation, we can see that the application of risk management techniques must follow the same principles. In this way, ERM will add practical value and help public sector managers and staff clarify and achieve their goals.

_____

[1]See: "Challenge - Getting a New Application Up and Running" Vol. 13 No.1; and "Province of BC: In the Vanguard of Enterprise-wide Risk Management" Vol. 12 No. 3. of At Risk.

[2]See RMB InTRAnet site:
http://www.min.fin.gov.bc.ca/PT/rmb/erm/ermTools.stm

[3]See discussion of the M. & S. model and others in Ryan, Neil "A comparison of three approaches to program implementation" in *International Journal of Public Sector Management*, Vol 4 No 9 1996.

E

R

M

Water, Water, Everywhere - Mop It? Yes...but THINK

Water is the most frequent and most costly cause of damage to government buildings and contents.

The cost to repair water damage is often much higher than it needs to be, solely because the remediation effort is not well thought out. Usually, this is due to a lack of knowledge, so in this article we will provide you with information intended to eliminate some of the most common and costly errors.
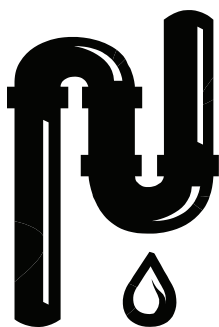
Water damage can result from the failure of a drinking water, sprinkler, drain or sewer pipe, from roof leaks, seepage of ground water and flooding. Water is particularly troublesome. It travels easily, is lead by gravity and is capable of fitting through the smallest openings. Even a small quantity can lead to big problems, not only from water itself, but from fungus (dry rot, mould and mildew), rust, corrosion, and water-born pathogens. In some cases, there are health issues in addition to property damage. In all cases, the damage is time sensitive. A prompt and appropriate response will always reduce damage and cost.

The most common error we see is underestimating the severity of damage. Even if it is clean, it may not be "just a little water" to be mopped up. If your paper files are saturated; if water is trapped inside walls or ceiling spaces (especially those with insulation); if it is in carpeting or any other substance or area which will dry slowly, you have a problem. Mould growth can become significant in as little as 24 hours. When it does, health risks and remediation costs go up. Drying quickly is the key to avoiding larger problems later on. Putting out a couple of fans is usually not good enough. Water damage restoration experts will often locate hidden water by using electronic moisture sensors, then use dehumidifiers to speed the drying rate. They may even make holes in walls, ceilings or cabinets to force drying air through enclosed spaces, or tear out carpet underpads to save the carpets; they may remove valuable items to be freeze dried off-site – all with the aim of reducing the overall cost. A more severe approach will be required when the water contains pathogens, or other harmful contaminants. Choosing the best remediation technique is difficult and requires considerable expertise.

Sometimes, out of an abundance of caution, the severity of the situation is overestimated. The mere possibility of mould leads to panic and an overzealous response. This can result in huge bills for tearing out and reconstructing areas that turn out (after lab analysis results are known) to have been only minimally contaminated, or not at all. Be aware that most building components and contents items –even computers and other electronics - can be saved with prompt, appropriate and cost-effective methods.

It is important to develop the right response and it is important to do it quickly. The specific response will depend upon the amount of water, the type of water (clean, grey or black/sewage), the types of material affected, the types and amounts of any moulds or pathogens and their locations relative to population risk groups (those with compromised immune systems are at highest risk).

Finally, is an error often seen in large organizations – the assumption that someone else will deal with it. This is common with Ministry employees, who assume that the landlord (usually Accommodation and Real Estate Services (ARES) - a division of Shared Services BC within the Ministry of Labour and Citizens' Services) will take care of damage to Ministry owned property. They won't.

So…Do It Right and Do It Fast. Make sure that someone with the required expertise is called in immediately. If you don't know who to involve, call Risk Management Branch at (250) 356-1794, anytime. In the meantime, stop the spread of water and start a basic mop-up using staff or a reputable restoration contractor.

Mop it? Yes…but THINK

Pandemic Preparedness

Early and thoughtful planning by organization management can reduce the impacts of pandemic influenza, protect clients and staff, protect essential services and minimize financial losses for the organization over the long term. Every organization will benefit from applying a number of key principles to planning efforts:

- Organizations that have access to **reliable data** will understand what to do. In particular, information available through websites maintained by regional health authorities and the Provincial Health Officer address the nature of the virus and the value of specific interventions.

- Internal monitoring of illness (**surveillance**) will be important to track employee absenteeism and to help plan immediate operational decisions.

- Offering **awareness and education sessions**, brochures and other materials in cooperation with local health authorities will help employees respond to the influenza threat with reason instead of fear.

- Strict adherence to **hand-washing** protocols is the cornerstone of an infection countermeasures plan and may be the most successful preventative action during a pandemic (even prior to deal with other types of infectious diseases).

- Informing and protecting the workforce will help avoid interruptions in essential functions, and may be the most important step any organization can take in managing pandemic risk.

- Information materials on protecting employee health are available on the Provincial Health Officer's pandemic website at:

  www.healthservices.gov.bc.ca/pho/pandemic.html

- Keep your organization functioning by understanding **essential functions** and know who are your **key players** and their required **skills**. Consider succession planning, cross-training and alternative ways that employees can work (e.g. teleconferencing, telecommuting, replacement workers, retired workers or contractors).

- **Collaborate** with other community members and stakeholders. It is worth the effort to check assumptions and let others know your intentions and expectations. Consider making connections with the following:

  ◊ Employees, unions, occupational health and safety committee;

  ◊ Significant Client organization;

  ◊ Suppliers and service providers;

  ◊ Regional Health Authority i.e. the local Medical Health Officer;

  ◊ Local government, especially the emergency program office.

Security - Works for me!

A tidily groomed young man was found making tea for himself in the lunch room of a government office. An alert staff member ascertained that he was not an employee or a guest. How or why the man gained entry to a secure building remains a mystery, but it was later confirmed that he is known to police.

Security is much more than screening by a guard at a point of entry. It is a "culture" of mutual support! We are all placed at risk when security fails, and we can all be part of the solution. The old wisdom that "*many hands make light work*" applies well to security and it is not an onerous task when we all pitch in.

Another man, injured some years ago, was enraged by an unfavourable ruling from an arbitrator. He threatened to come back to the office and "*make someone pay!"*. Implementation of pre-planned security responses afforded quick protection for the affected staff.

Just as observance of the '*rules of the road'* protects road users, we are protected by well understood and implemented security policies. Even good drivers can be placed at risk by the errors or carelessness of others. We collectively share the costs of required emergency responders, hospitalization, rehabilitation, and higher insurance costs.

When security fails we all pay. In addition to the extra work created by a loss, budgets that could be better used have to be expended to replace stolen, lost or damaged property.   Our best protection is a good understanding and application of the security policy.

BASED ON POLICY
The benefits of having a security management program are predicated on well written security policies (a roadmap to effective security)*.* Not only do security policies establish the requirements and roles for security across the organization, it provides a basis for developing standards and effective practices.

Ministries, under the direction of deputy ministers, are responsible for initiating, developing and implementing ministry-wide security management programs. Deputy ministers, senior managers and ministry security officers in each ministry collectively must manage security programs in their ministry, in accordance with policy from the Core Policy and Procedures Manual (http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/15_Security.htm). Using RMB security standards and guidelines the ministry security awareness program must be made understandable and real to all employees.

DELIVERY
Demonstrated support for security by leaders in an organization is vital in delivering an effective security message and program – especially when a change in procedures is required.

Orientation of new employees about security policies starts them out right, avoids the adoption of bad habits, and builds the security culture. Contractors and temporary workers should also be made aware of your security requirements.

Just as security vulnerabilities and loss experience change, security awareness needs to keep up. Security policies should be ever evolving and improving, which leads to the ongoing need for awareness training. Since good security involves everyone, and focuses on the overall enterprise, ongoing awareness and training is critical. Each update is an opportunity to energize the security culture.

Security - Works for me! (cont.)

It's not enough to rely on past success or luck. The security awareness program needs to be continuous, up-to-date and relevant to be effective. Whether the message is delivered by personal presentations, newsletter articles, posters, bulletins or word of mouth the messages must be consistent.

BRINGING IT HOME
Personal security and safety in the workplace are critical components of the security awareness message. Responsibility for security is shared, and we owe it to ourselves and to our colleagues. Effective security provides multiple benefits and safeguards employees, sensitive information, information systems, and personal and corporate property. The inclusion of security tasks and safe work behaviours in job descriptions will help advance the security program.

Training and education materials need to be relevant for the level of awareness required by the different audiences in the organization. Security must be seen as a primary job function for everyone.

By integrating security within other risk management initiatives it will develop a culture of mutual support between the security mentors and the rest of the organization. Being involved in risk mitigation, business continuity planning, emergency preparedness, OSH and other safety programs, crisis management planning and risk management initiatives ensures that the strategic considerations are raised about security as decisions are made and not as an afterthought.

Enhanced security awareness produces real benefits and is a significant factor in the success of the overall security of an organization.

To find out who your ministry/agency security officer is please use the following link: http://www.min.fin.gov.bc.ca/pt/rmb/committee/memSEC.stm

About Our Organization...

To find out more about the Risk Management Branch and Government Security Office please feel free to check out the following link:

http://www.fin.gov.bc.ca/PT/rmb/index.shtml