Global Information Assurance Certification Paper

Improving the Management of Information Security in Canadian Government Departments:

Taking Lessons from the ISO/IEC 27001 Standard to Make Continuous, Incremental, and Enduring Improvements

G7799 Gold Certification

Author: Ken Fogalin, ken.fogalin@gmail.com

Advisor: Jim Purcell

Accepted: April 10, 2009

Abstract

Canadian federal departments must now meet a relatively new standard to protect their information and information technology (IT) assets. In 2004, the Government of Canada directed compliance with their renewed Management of Information Technology Security (MITS) standard. This standard established the requirements for IT security for all federal government departments. Compliance with the baseline safeguards is mandatory, as is the conduct of a threat and risk assessment (TRA) to determine the necessity for additional safeguards. While the Government issued clear requirements, they offered little in the way of implementation guidance - departments are responsible to put this standard into operations. Not surprisingly, four years later, many departments are still struggling to achieve full compliance with this standard. Departments are also struggling to live up to the standard's management-level expectations. To be more specific, departments are struggling to establish an effective information security program; implement broader risk management activities; and continually improve to meet evolving threats. Fortunately, the ISO/IEC has published their eagerly awaited ISO/IEC 27001 Information Security Management System (ISMS) standard specifically to address these kinds of management problems. This standard has achieved worldwide acclaim and it is widely accepted as an indicator of a "good" information security program. For these reasons, this standard is a valuable benchmark against which Canadian federal departments could measure their own effectiveness. Departments could also learn proven methods to integrate their risk management activities, and time-tested security management processes to improve their own information security program. This paper will compare the Canadian MITS requirements against the ISO/IEC 27001 standard with these specific goals in mind. To complement these goals, this paper will also provide some practical steps-to-success to help departments close the gaps that they discover in making this comparison.

CONTENTS

1

INTRODUCTION

"Prime Minister criticized over data loss comment"

"Memory stick loss sparks government system shutdown"

"Liberal Democrats call for ban on memory sticks to carry confidential data"

"Recycled tapes yield data on former owners"

"Undetectable data-steeling Trojan nabs 500,000 virtual wallets"

INFORMATION INSECURITY IS MAKING HEADLINES

These were some of the stories that made headlines in a span of just a few days (October 30 to November 3, 2008). In fact, this is a very small selection of headlines from this timeframe. Consider that everyday there are similar headlines. Also, consider that everyday there are hundreds of similar incidents that do not make the headlines. If we follow the information security news for any length of time, we might deduce that our security practices are simply not good enough - we are doing a poor job of fending off the "bad guys." The evidence to support this grim outlook might come from the onslaught of network intrusions and escalading number of acts, standards, guidelines, and independent information security reports from public and private sector organizations. For example, Carnegie Mellon University's CERT Coordination Centre has reported that the number of information security incidents reported to them, by businesses, has doubled every year since 2000. We can see a similar trend in the information security literature, where the publications telling us how to secure our information and our networks have mirrored this growth (Conner, 2003). More recently, we might consider two more stories have made the headlines that specifically cite incidents on government systems.

"Number of reported cyber incidents jump"[1]

"Reported raids on federal computer data soar"[2]

These headlines claim that the number of reported incidents on government systems have increased by 40% since last year, and by threefold since 2006. According to one official, this dramatic rise in cyber attacks bears out that "Government systems are under constant attack."[3] We also need to consider that it is not always be data that attackers are interested in stealing. For example, the attacks on Estonia and Georgia show that undermining a nation's ability to operate was a primary motive (Cyber Security, 2008).

EVERYONE WANTS TO HELP – OR SO IT SEEMS

THE GOOD NEWS

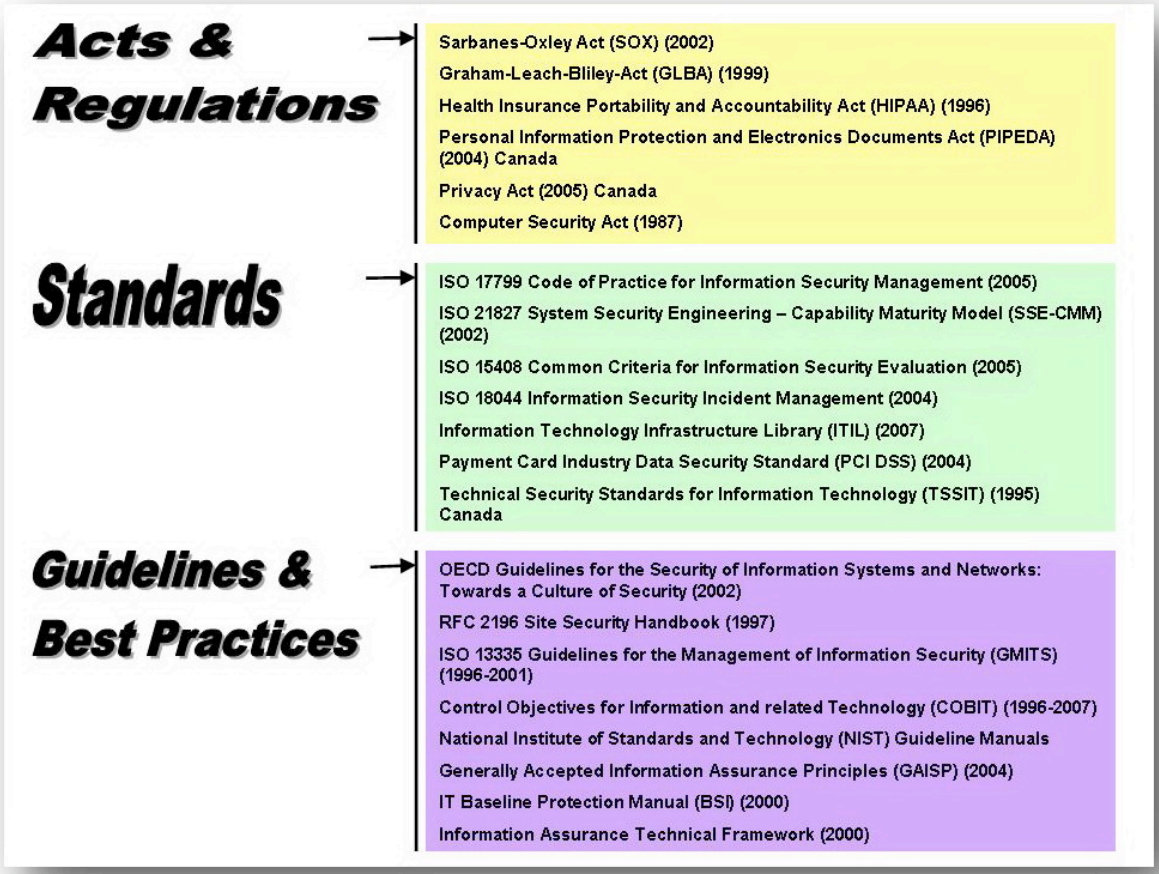
The good news is - we are not on our own to battle the growing number of ever-elusive attackers. We have an unwavering flow of new and evolving research, standards, and tools. This flow has already produced an abundance of legislation, regulations, standards, guidelines and best practices to help us protect our information and secure our networks (Figure 1). This growing collection of documents conveys our legal requirements and moral obligations, and illustrates the numerous controls we can implement. These documents, any many more like them, bombard our senior management with phrases like "due care," "due diligence," and "risk management." Some documents elevate information security concerns to the CEO and Board of Directors level, while others bombard our security management and security operations staff with yet another best practice to answer yet another threat that we should be concerned with.

[1] Story by Ben Bain, February 17, 2009. In Federal Computer Week

[2] Story by Peter Eisler, February 16, 2009. In USA Today

[3] Quote by Joel Brenner, counter-intelligence chief in the Office of the Director of National Intelligence. Reported in USA Today, February 16, 2009.

Figure 1. A glimpse at the prevailing regulatory, legislative, standards, guidelines, and best practice documents in the information security domain.



THE BAD NEWS

The bad news is – this influx of research and the resulting trail of documents, all contend for our precious time and resources. How do we decide which one(s) is best for our situation? They all profess to give us the protection we need. Yet in reality, they each target a specific problem area within the information security domain. Most of them focus on safeguards (in a checklist manner) and not on "activities." Most of them reflect the collective experience of the information security community and are therefore considered "best practices." By taking advantage of our "peer" experiences, we can implement these best practices and quickly improve within a specified area. However, these best practice documents tend to be very prescriptive leading us to believe that once we have "taken our medicine" we have nothing else to do (Richard A. Caralli, 2006). Yet, we can expect the bombardment to continue. For example, the U.S. Government is considering additional legislative action because many companies have

not sufficiently addressed (or may not be aware of) the laws that govern how they must address their information security needs (Conner, 2003). Furthermore, few of these documents have really helped us to view our information security program as anything other than an isolated cost centre buried deep within the IT Department. We still have no collaborative effort to link our information security program to the organization at large. Therefore, our compartmentalized approach leads to weaknesses and inefficiencies in security management. This in turn leads to unnecessary expenditures on security and possibly to serious exposure (ISACA, 2009). It is no wonder that the job of the Chief Information Security Officer (CISO) is one of frustration[4].

MOST OF US STUMBLE UPON GOOD INFORMATION SECURITY

OUR RELIANCE ON GOOD EXPERIENCE

Despite the bleak picture that this paper has so far painted for you, you should not deduce that your information security situation is wholly inadequate. Instead, you should realize that parts of your information security program are perfectly fine, while other parts probably need improvement. If you do have a good information security program (or believe you do), consider just for a moment, that you may have simply stumbled upon it. This is not meant to discredit your hard work in any way. Rather, the reason this statement has some merit is because many information security programs find their underpinning success in the good experience of the people implementing them – and not because of a disciplined repeatable approach comparable to industry standards (Arnason & Willet, 2008). We rely too often on the good experience of our people to overcome insufficient investments, fragmentation of security mechanisms, lack of integrated strategies, and professional qualifications (Chien Te-King, Hsu Wei-Chen, & Wang Mei-Fang, 2007). What is missing is a model that we can use to organize and talk about information security in management terms, rather than technical terms (ISACA, 2009).

[4] On August 11, 2008, Jill R. Aitoro wrote a story in GovernmentExecutive.com titled "Top IT cops say lack of authority, resources undermine security." This story expressed the frustration that government CISOs were feeling about their inability to take real control of their security requirements.

GOVERNMENT DEPARTMENTS ARE ALSO STUMBLING

Canadian federal government departments seem to be in this exact situation – they have stumbled upon information security that just might be "good enough." Some federal departments are even improving their IT security program, but any success is attributable to the experience of the good people that are implementing it and not to a formalized repeatable approach that is common among them. While most of us are still speaking in terms of threats, risks, controls, and technologies, our senior management is talking about cost, productivity and return on investment (ROI). Clearly, we need to change our approach and begin to speak in common terms because our current approach is wasteful[5] and hinders our ability to identify and mitigate cross-functional risk (ISACA, 2009).

THE GOVERNMENT'S QUEST FOR COMMON PROTECTION

Common protection among federal departments is what the Government of Canada had in mind when they put a stronger focus on information security in their renewed Government Security Policy. The Government clearly recognized that voluntary action would not be enough and they had to prescribe the minimum acceptable standards that federal departments must achieve. To achieve this common protection, the Government wrote their Management of Information Technology Security (MITS) standard telling their federal departments[6] "how to" organize and manage an information security program. However, the standard allows for flexible implementation[7] so departments can implement the standard in a way that is best for their particular situation.

[5] Organizational activities such as risk management, audit, compliance, privacy, business continuity, information security, and physical security all relate in some manner to security. We tend to view all of these as silos and do not typically connect them. They have different reporting structures, speak with different terms, and collectively may consume more organizational resources than necessary.

[6] For the purpose of this paper the generic term departments shall mean all departments listed in Schedule I, Schedule I.1, and Schedule II of the Financial Administration Act (FAA); any commission under the Inquiries Act that is designated by order of the Governor in Council; the Canadian Forces; and certain agencies and crown corporations that have entered into agreement with the Treasury Board of Canada Secretariat to adopt the Government Security Policy.

[7] Section 9 of the standard states that departments may differ in how they assign the required roles and responsibilities, but they must designate individuals to perform the required functions.

While the MITS standard did give departments the necessary governance framework for information security, many of them have failed to implement it to achieve its full effect. More specifically, the Auditor General of Canada has remarked that federal departments are struggling to establish an effective information security program, implement a consistent risk management strategy[8], and continually improve to meet evolving threats (Auditor General of, 2002). Since the Auditor General's audit in 2002, departments are making improvements, but it is not clear if these improvements are short-term reactionary fixes for a broken program, or long-term enduring improvements that are part of a strategic improvement plan.

THIS PAPER IS ABOUT ENABLING ENDURING IMPROVEMENTS

"The measure of success is not whether you have a tough problem to deal with, but whether it's the same problem you had last year." - John Foster Dulles

This paper looks at some of the struggles that Canadian federal government departments are facing and offers them a heartfelt solution. In Part I, this paper will postulate how federal departments arrived at this situation and what future pressures they may encounter. Then, in Part II, this paper will describe the standards that the international community is working from as their answer to the ongoing security management problem. In particular, this paper will focus on the process approach of the ISO/IEC 27001 Information Security Management System (ISMS) to point out how federal departments could benefit by changing their current ad hoc strategy for this more enduring approach. Then, Part III of this paper dissects the MITS standard and compares it to the prevailing ISO/IEC 27001 ISMS. The goal of this comparison is simply to demonstrate any noticeable gaps that federal departments should concentrate on first, to achieve some quick wins and gain some valuable momentum towards improving their current situation. Finally, Part IV of this paper provides some steps-to-success to help federal departments move forward and put the process principles of ISO/IEC 27001 into practice.

For those Departments that do not choose to adopt the ISO/IEC 27001 approach, this paper will at least serve as a resource for them. It will help them to understand the issues they are facing and to ask the right questions to implement a more effective information security program. It will help them to change the corporate mindset of "keep it up and running" to a mindset of "continuous operational improvement."

[8] More specifically, the Auditor General noted that departments conducted risk assessments only on an ad hoc basis, and those assessments focused on a single application or change to an IT system. The Audit was unable to find any evidence of that considered threats and risks to the department overall.

DISCLAIMER AND LIMITATIONS OF THIS PAPER

⚠ The comparison between the MITS standard and the ISO/IEC 27001 standard remains at high-level with respect to the concepts and requirements for establishing and managing an information security program. This is intentional to avoid any copyright violations or other infringement with respect to the standards reviewed in this paper. To show where MITS requirements match (or do not match) the standards as compared to the ISO/IEC standards, a bit of interpretation was required by the author. This interpretation is based on the understood intent of the MITS standard and the author's previous experience implementing the standard. No formal consultation took place with any current government official to help with this interpretation.

SUMMARY OF KEY POINTS

- ☑ The number and types of threats are growing at a rapid rate.
- ☑ Some attacks target our ability to operate rather than trying to steal our "secrets."
- ☑ We already have an abundance of research, standards, and other means to help us deal with the threats.
- ☑ The current regulatory and standards scheme focus on "checklists" and not activities that would better help us protect our networks.
- ☑ Most of us compartmentalize and isolate our IT security program deep within the IT Department and view it as a cost rather than an investment.
- ☑ We need a better means to overcome our weakness and inefficiencies in security management, and reduce unnecessary or misplaced expenditures on security.
- ☑ We do not have a model to organize and talk about information security in management terms vice technical terms.
- ☑ We rely on the good experience of our people to overcome insufficient investments, fragmentation of security mechanisms, and lack of integrated strategies.
- ☑ The Government of Canada has directed common protection among its federal departments, but departments are struggling to implement the Policy.
- ☑ Federal departments need a more enduring approach to achieve continuous improvement in the IT security program.

2

GOVERNMENT DEPARTMENTS' IT SECURITY STATE OF AFFAIRS

"Information security is hard. There ... I've said it." – Micki Krause

THE GOVERNMENT DEMANDS STRONGER SECURITY

The Government of Canada now has a stronger focus on information security. Their recently revised Government Security Policy (GSP) has laid down the law - federal departments must safeguard information systems by applying baseline security controls, continuously monitoring service delivery levels, tracking and analysing threats to their systems, and establishing effective incident response and continuity mechanisms. All federal departments must comply with the baseline requirements of the GSP and its associated operational standards and technical documentation. As well, departments must conduct their own TRA for every program, system, or service to determine the necessity of safeguards above baseline levels. This stronger focus on IT security demonstrates top-level support for national interests and the Government's business objectives.

PUTTING THE POLICY INTO OPERATIONS

COMMON PROTECTION IS A REQUIREMENT

The MITS is the Government's management-operational level standard that puts the GSP into operation. The MITS, published in April 2004, provides the safeguards to preserve the confidentiality, integrity, availability, intended use, and value of the information and IT assets held and controlled by federal government departments (Treasury Board of, 2004). It replaces the Government's nine-year-old Information Technology Security Standard (1995). The standard defines the baseline security requirements that federal departments must fulfill. These mandatory provisions set out to achieve consistency across the federal government for IT security and provide a minimum level of protection for all departments. At the very least, this ensures that all departments are managing the "known threats" that nearly every system is at risk from.

RISK MANAGEMENT REMAINS A PREVAILING THEME

One of the prevailing themes of the MITS standard is the risk management philosophy. This risk management philosophy recognizes that implementing all the controls in every department would be too costly and ineffective – so, senior

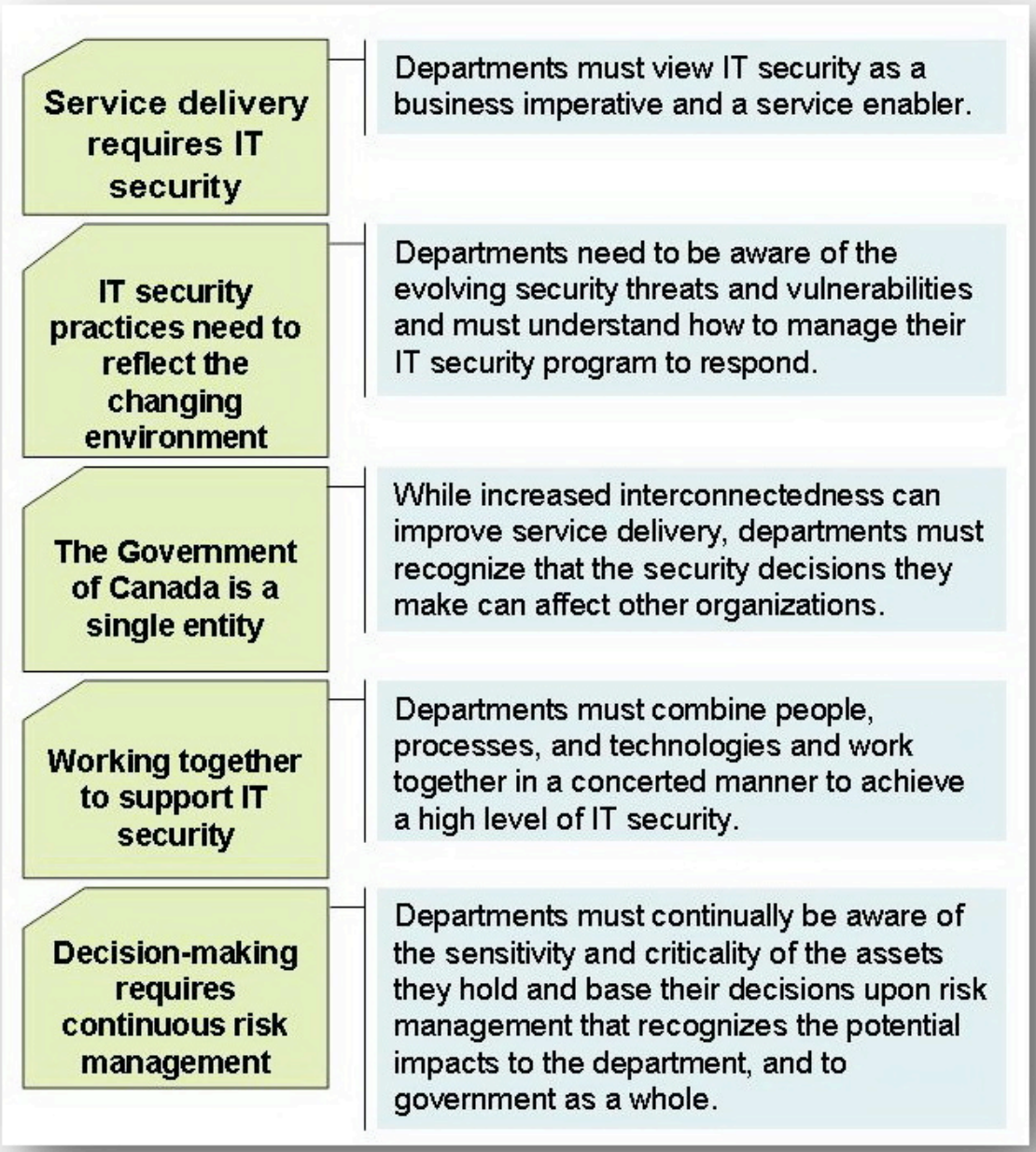
management has to accept a certain amount of risk. To assist in this regard, the MITS points departments to the Government's Integrated Risk Management Framework (IRMF). This is the Government's guide to assist senior management in their risk decision-making. Therefore, we might believe that by accepting a risk, senior management understands the risk and is therefore accountable, but this is not necessarily true. The reality is that the IRMF balances the departments' desires to exercise creativity and innovation and the Government's need to be prudent in the protection of its information[9]. This gives senior management sufficient freedom to form a different assessment of the risk or to exercise a different tolerance for a particular risk. As we might then expect, risk acceptance will be applied differently across departments. For example, a risk that is perfectly acceptable to Canada Post may not be acceptable to Canada Border Services or vice versa. This may not emerge to be a problem unless the two departments begin sharing information or infrastructure (weakest link principle). Since the MITS standard offers little in the way of implementation guidance, it is therefore open to interpretation. This leaves plenty of flexibility for individual departments to apply it based on their understanding of the intent and their own tolerance for risk acceptance. This might be a deliberately strategic move by the Government, because it means that departments can have different security solutions that are equally acceptable.

SECURITY PRINCIPLES ARE STILL IMPORTANT

The standard promotes some important security principles. While exercising their own tolerance for risk, these principles guide departments by prompting them to view information security as a business problem and not an IT problem, to think beyond their own boundaries, and to work together to enhance their security solutions. Figure 2 shows the security principles promoted by the MITS standard.

[9] Paraphrased from the Treasury Board of Canada Secretariat's Integrated Risk Management Framework.

Figure 2. Government of Canada Security Principles.



OPERATIONAL AND TECHNICAL CONTROLS ARE INCLUDED

The MITS standard spans the entire management-operational-technical scheme in one document. Part II of the standard gives direction and guidance on how to

organize and manage a departmental IT security program. This part includes the management controls such as roles and responsibilities, policy, resources, and risk management. Part III functions as the catalogue of operational and technical safeguards. This part presents a list of available safeguards within an active defence strategy, defined as, prevention, detection, response, and recovery (PDRR).

Under each of the PDRR headings, there are operational and technical safeguards, from which departments can select, to help them reduce their residual risk to an acceptable level. Both Part II and Part III include a mixture of "must" statements to ensure a minimum protection level, and "should" statements to allow for a graduated protection level based upon risk management. Overall, there are approximately 121 controls that departments must comply with (no risk decision required), and 32 controls that departments should consider. As you can see, the MITS standard, like the abundance of other standards we have, is heavily prescriptive.

THE GOVERNMENT ENCOUNTERS SOME DIFFICULTIES

"Any problem you can solve with a check isn't a problem, it's an expense." - Anonymous

THE 2002 AUDIT

The Government lacks operational and technical standards to implement the GSP. This is the criticism offered by the Auditor General of Canada in 2002. The MITS standard came nine years after its 1995 predecessor had been in force and not surprisingly followed shortly after the 2002 audit. The audit concluded that while the new GSP put a stronger focus on IT security, the operational and technical standards needed by the individual government departments to implement the Policy were outdated or did not exist.

The Government also has difficulties to identify potential gaps in the security of IT infrastructure across federal departments. This was another observation by the 2002 Audit Report, which noted that the Government does not have an adequate basis to determine whether current IT security practices are sufficient and appropriate. Furthermore, the Government does not have an appropriate baseline to measure future progress (Douglas G. Timmins, 2002). The audit further identified a number of issues that the Government needs to address to improve IT security across departments to meet the key security and privacy concerns previously identified by the Government-On-Line initiative (Auditor General of, 2002).

THREE YEARS AFTER THE AUDIT

Senior managers need to pay more attention to identifying threats and risks, developing action plans for correcting weaknesses, and ensuring that their departments are fully compliant with IT security policies and standards (Douglas G. Timmins, 2005). These comments came from the Auditor General of Canada three years later in a follow-up to the audit. In an opening statement to the Standing Committee on Public Accounts, the Assistant Auditor General stated that, in most departments, senior management "is not made aware of the IT risks, and therefore, may not attach sufficient priority to addressing them." This was not a new concern and it undoubtedly existed well before publication of the MITS standard (as suggested by statements in the 2002 Audit Report).

The Government has a noticeable less than stellar commitment to information security. Despite some encouraging signs of improvement, departments have not made satisfactory progress towards strengthening their IT security program since the 2002 Audit. The Auditor General of Canada, Sheila Fraser, said in her opening remarks to the Standing Committee on Public Accounts that she is "disappointed that the Government still does not meet its own minimum standards for IT security even though most of them have been well known for more than a decade." (Sheila Fraser, 2005).

THE GOVERNMENT IS BECOMING MORE INTERCONNECTED

Within the Canadian Government, information security may no longer the sole purview of the individual federal departments. In today's global on-line environment, digital information and IT assets are widely distributed and linked via the Internet or other communication means such as a dedicated backbone. In addition, the Government's On-Line Service Vision is looking to reduce federal program gaps, overlaps, cross-department confusion, and inefficiencies to provide more harmonized services to Canadians. For example, government departments ask Canadians repeatedly, to fill out online forms because the information they provide to one department or program is not re-used or shared with other departments or programs[10]. This wastes time and resources for all concerned and is driving the need for departments to become more integrated and federated.

One means of accomplishing these objectives is to implement more common and shared infrastructures to replace the currently prevalent "stovepipe" networks. Moreover, some federal departments already have, or plan to develop, links or

[10] This example is from the PWGCS Website Secure Channel project.

information sharing agreements with multiple "partner" businesses both nationally and internationally. This interconnectivity between government departments, non-government organizations, private industry, and international partners is developing into a dominant trend that is creating new opportunities for collaboration, but also introducing new risks (Auditor General of, 2002). Canadian federal departments have yet to understand its real impact within their information security program.

MORE INTERCONNECTIVITY CALLS FOR MORE ASSURANCE

"If we don't change our direction, we are likely to end up exactly where we are headed." - Anonymous

OUR RISK SHOULD NOT BE THEIR RISK

As more threats emerge and more interconnections develop, all partners involved may want even more assurance that we are using adequate privacy and security measures. Partners will seek assurance that any lack of security on our part will not put their information or their network at risk. Providing this assurance may be more complex than first glance suggests. After all, there is already an abundance of standards offering organizations, and even nations, plenty of operational and technical countermeasures to help secure the network and manage the ever-evolving threats and risks. Furthermore, computer scientists are continuing to develop technologies to support information security – and these technologies can even achieve an "Evaluated Assurance Level" (i.e., accreditation status) under the Common Criteria[11] standard. But, which standard will satisfy our "partners"? Canada has developed it own IT security standards, as has other nations, and has even harmonized its TRA methodology[12] to alleviate much of their intergovernmental disparity. However, it is unclear whether the government standards will give our interconnected "partners" the level of assurance that they may be seeking.

[11] ISO/IEC 15408 Common Criteria for Information Security Evaluation (2005)

[12] Harmonized Threat and Risk Assessment Methodology (2007). Joint Publication by the Communications Security Establishment and the Royal Canadian Mounted Police

THE EROSION OF CONFIDENCE IN OUR STANDARD

Furthermore, the growing number of headlines pointing out our insecurity may cause worldwide trust in our nation's standards to erode. For example, Canada's Privacy Commissioner, Jennifer Stoddart, has also made the headlines. She said at a conference that Canada is getting a global reputation for its lax legislative environment with respect to cybercrime and its inaction is an embarrassment for a country that prides itself on protecting rights and maintaining high standards of living. The Privacy Commissioner noted that Canada does not have adequate provisions for anti-spam, identity theft fraud, or data breaches and is beginning to show up alongside other hot spots (such as Nigeria) as a source of Internet attacks. Canada has simply fallen behind, and this threatens businesses, individuals and network providers (Gillian Shaw, 2008). If the headlines spark a non-confidence movement towards a nation's standard, it follows that there may be a shift towards conforming to a universally recognized standard. Conforming to an accepted standard may indeed become regarded as the "norm" and may turn out to be the required proof that we have implemented a "good enough" information security program.

THE ISO/IEC SAYS CONFORMITY IS GOOD BUSINESS PRACTICE

The ISO/IEC embraces the point-of-view that adopting a universally accepted standard is, without question, a good business practice. To this end, they are developing and promoting a uniform understanding of the terminology, concepts, intent, and application of information security standards. The ISO/IEC is midstream in the production of a relatively new set of information security standards, focused at the management level, specifically to resolve this conformity problem. The standards are grouped into what is known as the 27000 family of standards. This family of standards is the topic of Part II of this paper.

REAL QUESTIONS WE NEED TO ANSWER

The Leadership within Government has put stronger focus on information security. The Auditor General has urged senior management to take responsibility and put this stronger focus into operations. To direct and guide their federal departments, the Government has published (renewed) their IT security standard. However, many departments are struggling simply to comply with their Government's direction and certainly making continuous improvement within information security program seems to be eluding many of them. Nevertheless, let us assume that the federal departments can indeed fully implement the MITS standard. The questions that follow are, "Is it good enough?" and "Does compliance with the MITS standard mean federal departments have a good information security program?" Obviously, there are no easy answers to these questions, but there is a means of helping federal departments formulate some. To this end, this paper compares the MITS standard to the prevailing international standard for information security management.

SUMMARY OF KEY POINTS

- ☑ The Government of Canada now has a stronger focus on information security. Their mandatory provisions set out to achieve consistency across the federal government for IT security and provide a minimum level of protection for all departments.
- ☑ Risk management is still a prevailing theme, but it does not hinder our freedom to form a different assessment of the risk or to exercise a different tolerance for a particular risk.
- ☑ The Auditor General of Canada (in 2002) has criticized the Government and its federal departments for lacking an appropriate baseline to measure future progress.
- ☑ Despite some encouraging signs of improvement, departments have not made satisfactory progress towards strengthening their IT security program since the 2002 Audit.
- ☑ Departmental senior managers need to pay more attention to identifying threats and risks, developing action plans for correcting weaknesses, and ensuring that their departments are fully compliant with IT security policies and standards.
- ☑ The growing interconnectivity between government departments, non-government organizations, private industry, and international partners is developing into a dominant trend that is creating new opportunities for collaboration, but also introducing new risks.
- ☑ As more threats emerge and more interconnections develop, all partners involved may want even more assurance that we are using adequate privacy and security measures.
- ☑ Canada's Privacy Commissioner says that Canada is getting a global reputation for its lax legislative environment with respect to cybercrime. Canada has simply fallen behind.
- ☑ The ISO/IEC is midstream in the production of a relatively new set of information security standards, focused at the management level, specifically to provide a common baseline from which we can all work.

3

THE STANDARDS OF THE INTERNATIONAL COMMUNITY

"The unexamined life is not worth living." - SOCRATES

Think about this quote in regards to your information security program. In times of fiscal constraint, an unexamined program is not worth funding. It should not surprise us then, when senior management cuts our security budget or simply brushes off our latest "scare tactic." Yes, senior management understands that information security is an imperative. However, that does not mean that they should permit it to function with any less rigour than any other business imperative. Part II of this paper describes a set of standards that will give you the methods you need to not only examine your information security program, but also to continually examine it, and to manage it with the rigour necessary to optimise the use of your resources (people, money, time). However, it will require that you shift your thinking from the "checklist" to the "processes" behind checklist.

THE NEED FOR A NEW SET OF STANDARDS

"There Is Always A Right Way and A Wrong Way to Succeed"[13]

A FAMILY OF STANDARDS

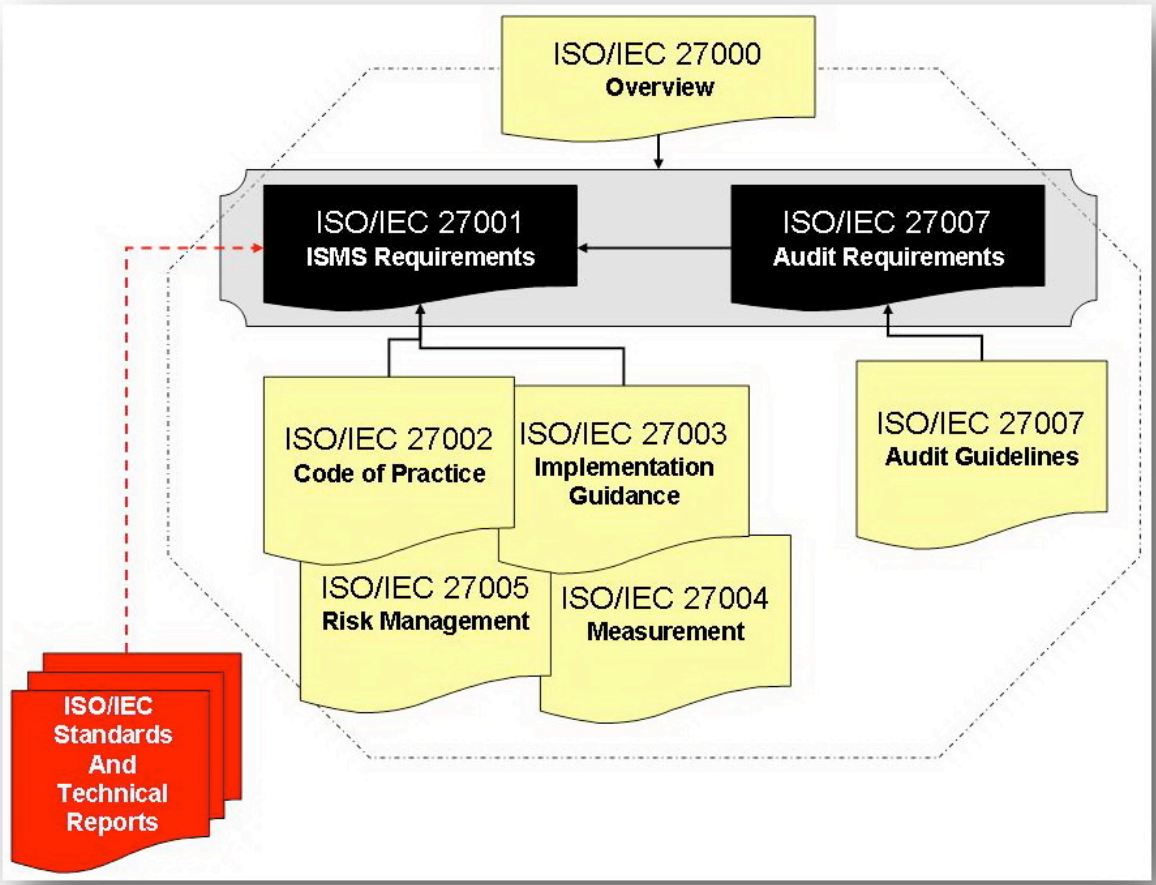
We are all very comfortable implementing operational and technical level safeguards, but far less comfortable with the management safeguards. Only recently have we seen more literature discussing the management aspects of information security. However, we have not seen any real global consensus on the "right way" to manage our information security programs.

The ISO/IEC is trying to change this. They have devoted considerable effort to bringing us a relatively new set of standards dedicated to the management of

[13] Two Jesuit priests both wanted a cigarette while they prayed. They decided to ask their bishop for permission. The first asked but was told no. A little while later, he spotted his friend smoking. "Why did the Bishop allow you to smoke and not me?" he asked. "Because you asked if you could smoke while you prayed and I asked if I could pray while I smoked!" the friend replied.

information security. The ISO/IEC 27000 family of standards consists of a number of inter-related standards (some of which are not yet published) that endeavour to give us the consensus we need. The relationship between these standards is shown in Figure 3. The main pillar of the family (ISO/IEC 27001) specifies the requirements of an information security management "system" and forms the basis against which we could achieve "recognition."

Figure 3. The ISO/IEC 27000 Family of Standards.



FAMILY SUPPORT

The 27000 family of standards might not fulfill all of our security needs. Therefore, the ISO/IEC maintains a long list of issue-focused standards and guidance documents. While these standards sit outside the family, they do provide us with further in-depth knowledge on specialized topics such as incident handling, network security, disaster recovery, and trusted third party services, to name just a few. Table 1

shows a partial list of the well-known standards that directly support the 27000 family of standards.

Table 1. ISO/IEC standards and technical reports that support the 27000 family of standards

Standard
ISO/IEC 18028-1 Information technology security techniques – Part 1 – Network security management
ISO/IEC 18028-2 Information technology security techniques – Part 2 – Network security architecture
ISO/IEC 18028-3 Information technology security techniques – Part 3 – Securing communications between networks using security gateways
ISO/IEC 18028-4 Information technology security techniques – Part 4 – Securing remote access
ISO/IEC 18028-5 Information technology security techniques – Part 5 – Securing communications across networks using virtual private networks
ISO/IEC 18043 Guidelines for the selection, deployment and operation of intrusion detection systems
ISO/IEC 24762 Guidelines for information and communications technology disaster recovery services
ISO/IEC TR 13335-1 Information technology guidelines for the management of IT security – Part 1 – Concepts and models for IT security
ISO/IEC TR 13335-2 Information technology guidelines for the management of IT security – Part 2 – Managing and planning IT security
ISO/IEC TR 13335-3 Information technology guidelines for the management of IT security – Part 3 – Techniques for the management of IT security
ISO/IEC TR 13335-4 Information technology guidelines for the management of IT security – Part 4 -Selection of safeguards
ISO/IEC TR 13335-5 Information technology guidelines for the management of IT security – Part 5 – Management guidance on network security
ISO/IEC TR 15947 Information technology intrusion detection framework
ISO/IEC TR 18044 Information security incident management

THE HEAD OF THE FAMILY

"If I have seen further, it is only by standing on the shoulders of giants" – Sir Isaac Newton

ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

In 2005, the ISO/IEC published this eagerly awaited standard to specify the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a good[14] Information Security Management System (ISMS). While the ISO/IEC's Joint Technical Committee definitely advanced the standard, it would be unfair to say they developed it. In 2002, the British Standards Institute published their BS 7799-2 standard. This standard began to influence the rest of Europe and even got some worldwide attention. Later the ISO/IEC took an interest and eventually took over the BS 7799-2 standard and used it as the basis for producing their ISO/IEC 27001. The ISO's Joint Technical Committee took input and feedback from a consortium of companies to ensure this standard would meet industry needs. Because of this approach, the standard has received international recognition. According to ISO's directives, to be internationally recognized, a standard requires approval by at least 75 percent of the national participating members[15]. Therefore, this standard represents the consensus of a considerable body of expertise. Although this standard had some history (it was not a complete surprise), the information security management community still perceived the official release of ISO/IEC 27001 as a big event. The main reason for this is that the ISO/IEC put together the best practices in information security with a hugely successful four-step process approach[16], known as the Plan-Do-Check-Act (PDCA) cycle. Not coincidently, this is a robust model for

[14] A good information security program is one that is formed on industry-accepted practices.

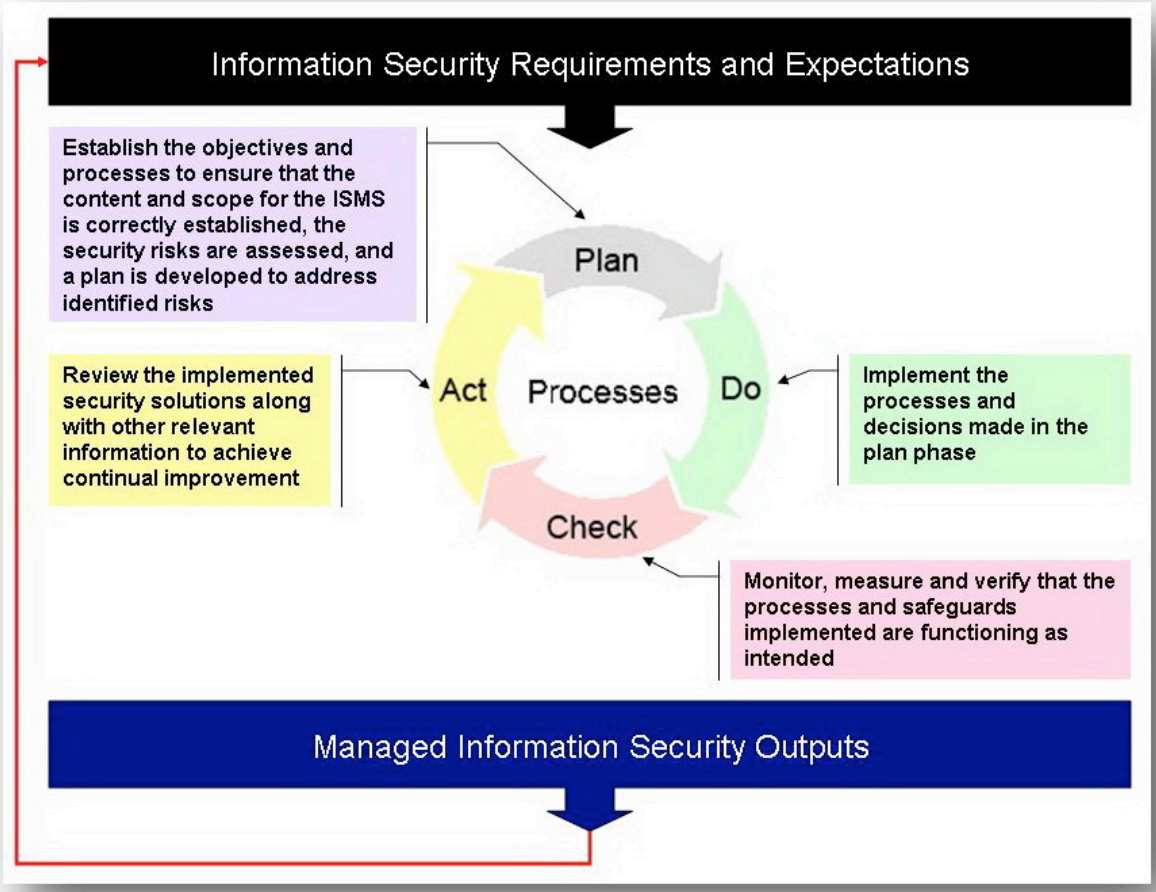
[15] Canada is a participating member of the ISO/IEC JTC 1/Sub-Committee 27 - Information Security Techniques. Participating members have an obligation to take an active part in the work and to vote. There are 24 participating members in this sub-committee. In addition, there are 12 observing members in this sub-committee. Observing members have the option to take an active part in the work, but do not have any voting privileges.

[16] The ISO/IEC considers a process approach to be the application, interaction, and management of a system of processes to achieve information security vice a checklist of controls to be put in place. Processes take security requirement inputs from stakeholders and through some action(s) produce information security outcomes that meet the requirements and expectations of those stakeholders.

implementing the principles set out in the 2002 OECD Guidelines[17] governing security risk assessment, security design and implementation, security management and reassessment for information systems and networks. Figure 4 graphically illustrates this process improvement cycle.

[17] On November 26, 1992, the Organisation for Economic Co-operation and Development (OECD) published its landmark Guidelines for the Security of Information Systems report. This report fell out of the need to address the potential threats to information systems that cross national boundaries. Therefore, a group of experts from 24 OECD member nations gathered to produce suitable recommendations. Ten years later, the OECD recognized that the use of information systems and network has dramatically changed from what they wrote about in their 1992 guide. Therefore, in 2002, the OECD republished their recommendations under a new report titled Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. The aim of this guide is to promote a culture of security; raise awareness of risks; and promote co-operation in the development of information security policies, practices, and procedures. The nine principles of the 2002 version include awareness; responsibility; response; ethics; democracy; risk assessment; security design and implementation; security management; and reassessment. The OECD guide provides an ideal forum for nations to agree on very broad principles of information systems security.

Figure 4. The ISMS Process Improvement Cycle.



A working example might be useful to appreciate this model[18]. The company's stakeholders may provide an input for an information security requirement such as – **breaches of information security must not cause serious financial damage or embarrassment to the organization.** The stakeholders could also provide an input for an expectation such as – **if a serious incident does occur, there should be people with sufficient training and appropriate procedures to minimize the impact.** Following

[18] Working example requirements and expectations statements are taken from the ISO/IEC 27001 standard.

this example through the model, the security management team would take these two inputs through the PDCA cycle.

In the "Plan" phase, they would identify the potential risks, articulate the legal requirements, and establish the responsibilities, resources, controls, risk acceptance criteria, and procedures needed to prevent breaches and manage them when they do occur. After completing this phase, the team would seek senior management approval for the residual risk and obtain authorization to implement their plan – i.e., move to the "Do" phase. The "Do" phase enables the security management team to implement the plan and manage the day-to-day security operations. The "Check" phase would include activities such as detecting an attempted or successful breach, determine how the breach occurred and how it was handled, review and measure the effectiveness of the controls in place taking into account any changes to the company's organizational structure, people, processes, or technology, and finally update their plan. The final set of processes, "Act," is when the security management team would apply the lessons learned from this experience, implement the necessary improvements, and communicate their actions and improvements to the interested stakeholders to ensure it satisfies their requirements.

Obviously, this is a very simplified account of how the PDCA processes might work for any requirement and expectation. The ISO/IEC 27001 standard provides guidance that is much more detailed. In addition, there are a growing number of valuable resources available through consulting companies, seminars, and book publishers. Alternatively, you may prefer to think about this process approach using another acronym. The Quality Digest has proposed the acronym 4P, meaning, Prepare, Perform, Perfect, and Progress[19].

A PROVEN PROCESS IMPROVEMENT MODEL

"Why climb the corporate ladder when you can take the elevator?"

The PCDA process-approach is the core of the standard. This is the same process-approach used by other long-standing and distinguished management systems such as ISO 9001, the standard for Quality Management, and ISO 14001, the standard for Environmental Management Systems. Dr. W. Edwards Deming, who many consider the father of modern quality control, made the PDCA cycle popular initially within the manufacturing sector. At first, many organizations ignored his process-

[19] Acronym 4P proposed by Praveen Gupta in online version of Quality Digest (2005) http://www.accelper.com/pdfs/From%20PDCA%20to%20PPPP.pdf

based approach, but after the rapid rise in product quality in Japan, most organizations began to embrace it. The concept caught on under the "Total Quality Management" movement and has since been successfully applied to many other environments. For example, being ISO 9001 or ISO 14001 compliant is a highly sought after certification by organizations worldwide as the mark to distinguish themselves as a quality company. Not surprisingly, the worldwide total for ISO 9001 compliant companies approaches 1,000,000 across 175 countries with China leading the way (210,733 certificates) and for ISO 14001 there are 154,572 compliant companies in 148 countries again with China leading (30,489 certificates). The United States and Canada have also embraced both of these standards – the United States has 36,192 ISO 9001 certificates and 5,462 ISO 14001 certificates making it into the top ten countries – Canada has 7,462 ISO 9001 certificates and 1,066 ISO 14001 certificates.

Now, the ISO/IEC has applied this same conceptual management system model to the discipline of information security. If early numbers are a valid indicator, then ISO/IEC 27001 is beginning to achieve similar success. According to the International Register of ISMS Certificates[20], the total number organizations certified against the standard is already 4,987 across 73 countries – with a growth of 1,935 for the year 2007 alone. Japan leads all other countries with 2,863 certified companies, followed by India (433 certificates), Britain (368 certificates), Taiwan (202 certificates), China (174 certificates), Germany (108 certificates), and the United States (82 certificates). Canada has two[21] certificates indicating that some companies understand the value of being ISO 27001 compliant. Although the expertise within Canada exists only minimally right now, we should expect this trend to grow.

THE PROMISE OF THE PROCESS IMPROVEMENT APPROACH

The process approach promises to achieve the sought after results more efficiently because the activities and the resources are managed as a process. This approach offers a number of key benefits such as improved, consistent, and predictable results; and the possibility to focus and prioritize improvement opportunities[22]. The process approach helps us avoid the treating our "sore spots" with short-term fixes to symptoms, and instead look for long-term cures to the problem themselves (ISACA, 2009). However, organizations generally spread processes across functional

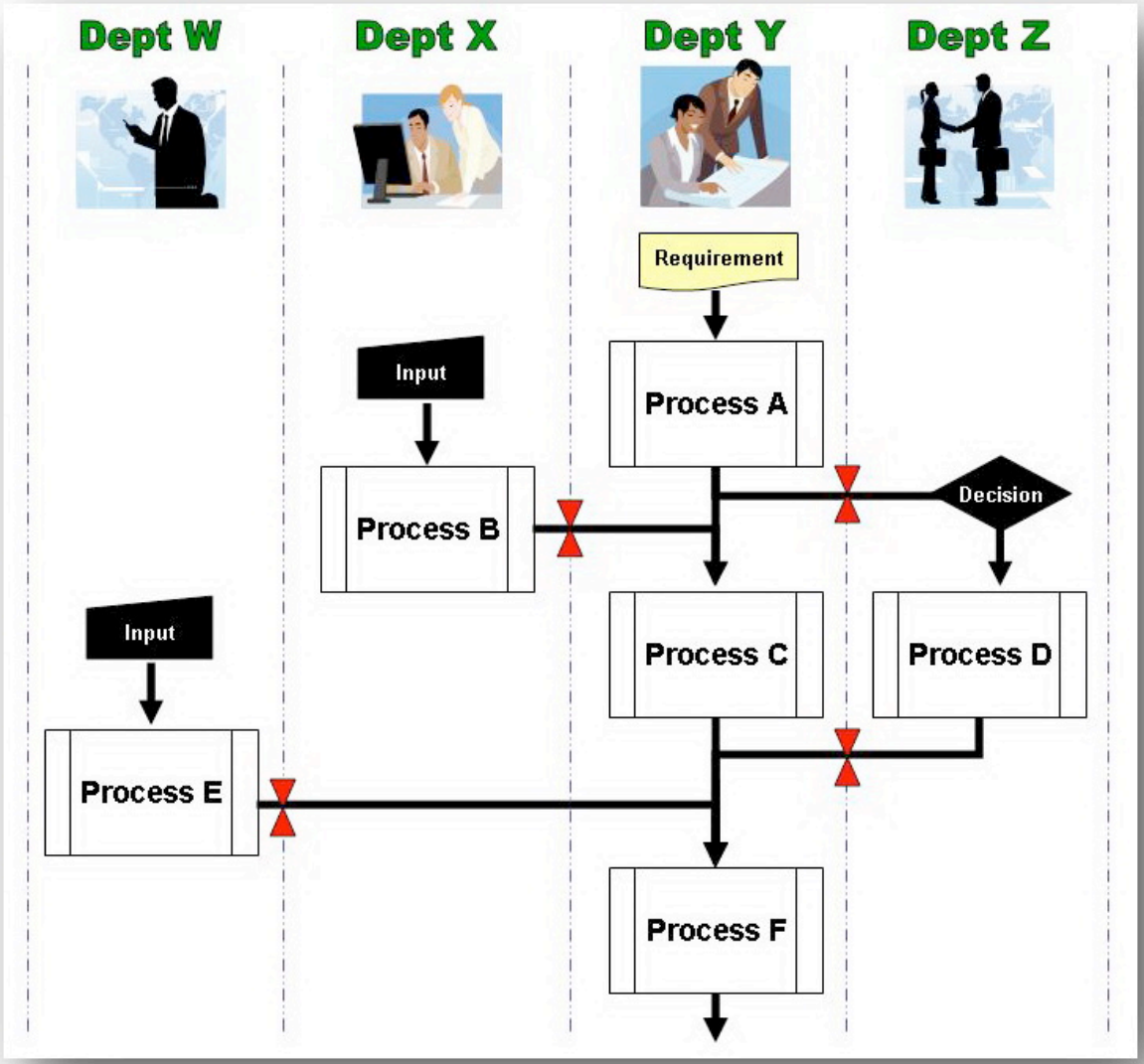
[20] http://www.iso27001certificates.com

[21] The two organizations in Canada that are certified ISO/IEC 27001 compliant are Axalto Canada, and Research in Motion.

[22] Benefits derived from ISO 9000 / ISO 14000 Quality Management Principles

departments – no one department owns all the processes that contribute to the company's overall objective. Therefore, to realize both effectiveness and efficiency, we need to identify related processes and manage them within a systems approach. This systems approach will help us understand the interactions and consequences of addressing only a particular issue, and will achieve the integration and alignment that best brings about the desired results. Figure 5 illustrates this orchestration.

Figure 5. A view of functionally owned processes and their relationship within a systems approach.



A walkthrough of how incident management might work in a large department will provide a good example of how the systems approach works. In this example,

Dept Y is responsible for managing incidents and has the ultimate responsibility to ensure the stakeholders' requirements and expectations are satisfied. However, Dept W owns and monitors the intrusion detection systems that may trigger an incident report, and Dept X runs the national help desk that may receive an incident report from a user. Both Dept W and Dept X follow their established processes, based on the priority their Dept Head has established and the resources allocated to them. They complete their process and pass off their results to Dept Y to manage the incident. At some point in the overall process, Dept Y may request a risk decision from Dept Z. Dept Z follows its established process and returns a decision to Dept Y to carry on managing the incident. The process may end with an incident investigation or root cause analysis and the lessons captured. In a successful case, Dept Y communicates the result to the stakeholders to reassure them that the incident management process has met their requirements and expectations. If the process needs improvement or the requirements and expectations have changed, Dept Y coordinates and leads the process improvement method (PDCA) with membership from Departments W, X, and Z.

The potential problem with this approach is that functional departments focus on their priorities and give less priority to the problems that occur at the interface boundaries – leading to little or slow improvement for the organization as a whole (ISO, 2004). On the positive side, this approach brings about better management and control of the processes and interfaces between the functional departments of the organization (ISO, 2004).

To make this work we need to think in terms of how our work affects the quality of the processes that follow. In other words, process thinking generally draws on multiple functional skills. The result is a push for higher quality inputs and outputs each time processes intersect (Curt Fleming, 2002). Therefore, the PDCA approach is a powerful way of introducing horizontal management that crosses the barriers of functional units and unifies their focus on the desired organization-level goals leading to greater value for our client (ISO, 2004). In other words, IT security processes become enabling processes (i.e., their clients are within the organization) (Wim P.M. Vanhaverbeke & Huub M.P. Torremans, 1998). This approach also provides suitable "at-a-glance" outcomes that senior management likes to see.

RISK MANAGEMENT IS STILL CORE FEATURE

Risk related activities are another core feature of the ISO/IEC 27001 standard and it tightly integrates the use of risk assessment and risk management methods into

the PDCA process activities. Although the standard does not specify that we use a particular risk assessment method, it does specify a number of risk related requirements. For instance, before we proceed to identify the risks senior management must first: decide on the criteria that they will use to evaluate risk; agree to a risk assessment methodology[23]; and decide the criteria for accepting risk along with the acceptable risk levels. After identifying the risks, we must then evaluate options to mitigate the risks to the acceptable level.

While the application of controls is the preferred method to mitigate risk, it is not necessarily the only way to accomplished this. For example, other means for the treatment of risk could include accepting the risk, avoiding the risk, or transferring the risk (for example, to an insurer). However, the usual approach is the application of controls so the requirement naturally leads us to a catalogue of best security practices[24] as a starting point for the treatment of identified risks.

The ISO/IEC 27002 Code of Practice is the preferred source for the selection of controls to mitigate risk. However, it is important to understand that not all the controls in the catalogue are obligatory. We have complete freedom to exclude any of the controls with suitable justification. Furthermore, the list is not exhaustive (meaning that we may need to look elsewhere for additional controls), but it is comprehensive enough to ensure that we do not overlook important control options.

Finally, the standard requires us to obtain management approval for the residual risks, and prepare a "statement applicability" to provide a summary of the decisions concerning risk treatment and the justification for any exclusion. Overtime, as the organization, technology, or business objectives and processes change, the standard requires that we review the risk assessments, the residual risks, and the identified acceptable levels of risk.

THE FAMILY CATALOGUE

ISO/IEC 27002 CODE OF PRACTICE

In 2005, the ISO/IEC published the second edition of their international standard ISO/IEC 27002 Information Technology Security Techniques – Code of Practice for

[23] The standard refers to ISO/IEC TR 1335-3 GMITS for examples of risk assessment methodologies.

[24] This is a related standard – ISO/IEC 27002 – and is discussed in the next section.

Information Security Management. This standard gives us a catalogue of control objectives and controls that we should think about for the treatment of risks that we identify with our risk assessment and risk treatment processes (during the PLAN PHASE).

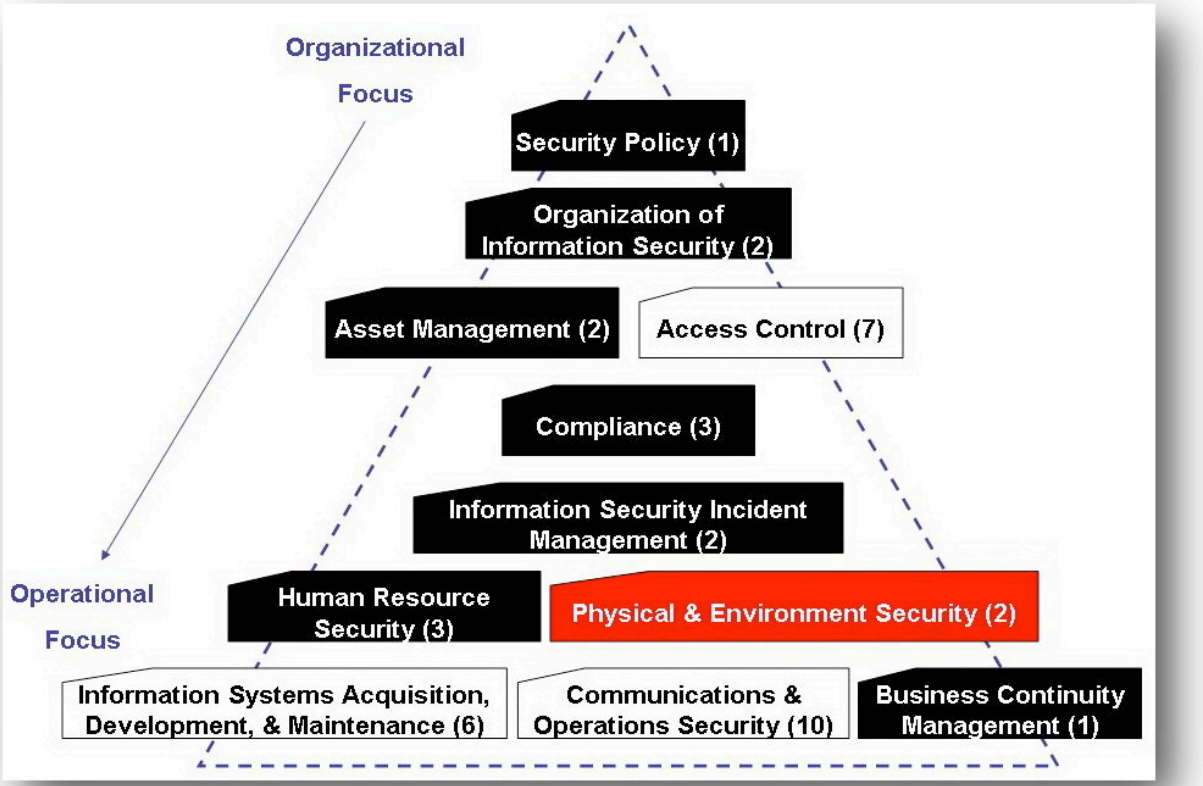
The history of the ISO 27002 standard dates back to 1993 when the Department of Trade and Industry in the United Kingdom first published their "code of practice." In 1995, the British Standards Institute (BSI) adopted this code of practice, labelled it BS 7799, and released it in two parts. In 2000, the ISO took charge of Part 1 of BS 7799 and renamed it to ISO 17799. In 2005, the ISO/IEC revised and reissued the standard to reflect the ever-changing risks, controls, and best practices relevant to information security management (International Organization for Standardization, & the International Electromechanical Commission, 2005).

While the ISO 27002 standard is essentially a generic advisory document, we should consider it a good starting point for implementing information security. The rationale for this is simple - the recommended controls represent common legislative requirements or widespread practices within the information security community.

HOW THE CATALOGUE WORKS

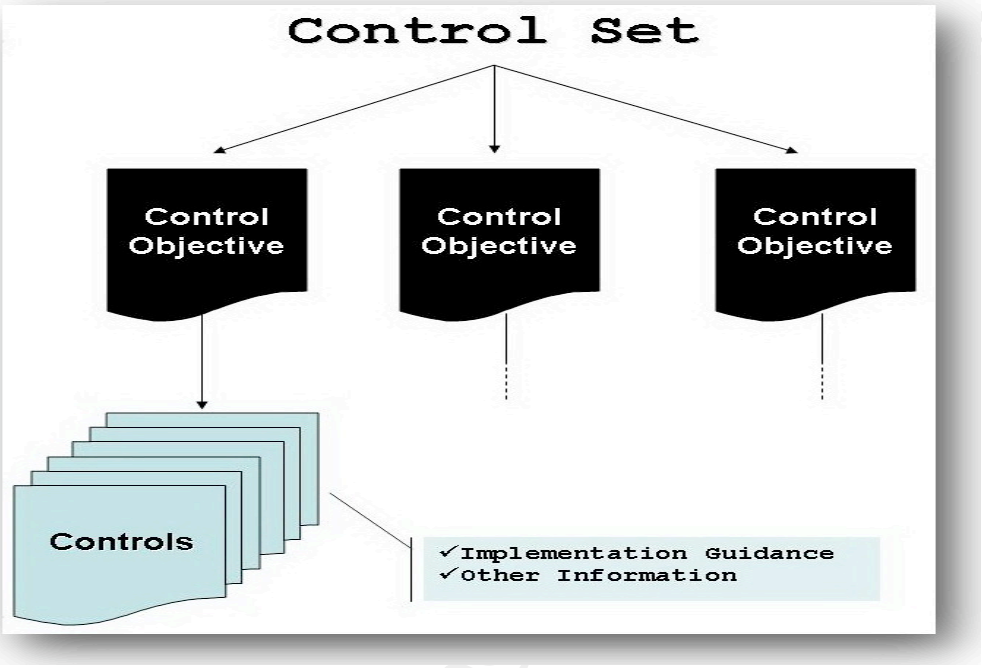
The standard contains 11 security "clauses" that cover a broad spectrum from our high-level organizational needs to our lower-level operational needs. Each security clause is further broken into control sets – 39 in all. Figure 6 illustrates the grouping of the security clauses with the number of their associated control sets.

Figure 6. Security clauses of the ISO/IEC 27002 standard.



The standard breaks down even further. Each control set provides its own control objectives (i.e., a statement of what is to be achieved). For example, under the control set "**Access Control**," one of the control objectives is "**to ensure authorized user access and to prevent unauthorized access to information systems.**" Finally, each control objective has its own controls that we can apply to achieve the control objective. Continuing our example, one control is "**there should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services**." The standard also gives us detailed implementation guidance and other information that we should consider. In total, the ISO/IEC 27002 standard lists 127 individual controls offering us a very comprehensive means of mitigating the risks they we have identified. Figure 7 graphically illustrates the relationship between these elements.

Figure 7. How ISO/IEC 27002 organizes and presents security clauses (i.e., control sets), control objectives, and controls.



STANDARDS IN HARMONY

The Code of Practice (ISO/IEC 27002) standard is difficult to separate from its overarching ISMS standard (ISO/IEC 27001). These two standards work in harmony. The ISO/IEC 27002 functions as the compliance catalogue so we can self-measure whether we have at least considered all of the controls. This in turn could lead to certification under the umbrella of the ISO/IEC 27001, but this is optional.

A GOOD FIT FOR ANY ORGANIZATION

The ISO/IEC 27002 standard provides such level of detail that it is ideal for organizations of any size and it would not be difficult to implement. Furthermore, the ISO/IEC 27002 is a technology-neutral standard, so we have plenty of flexibility to employ whatever technology we choose to achieve the desired control objectives. Even better, we do not have to achieve all of the control objectives or implement all of the controls to be compliant with the standard. The ISO/IEC simply requires that we select the controls we require based on our own unique security requirements so long as we have reduced our risks to an acceptable level and we have documented this appropriately (International Organization for Standardization, & the International Electromechanical Commission, 2005).

SUMMARY OF KEY POINTS

- ☑ We need to continually examine and manage our IT security program with the rigour necessary to optimise the use of your resources (people, money, time).
- ☑ We need to shift our thinking from the "checklist" to the "processes" behind checklist.
- ☑ The ISO/IEC 27000 family of standards gives us some consensus in the management realm of information security.
- ☑ The ISO/IEC 27000 family of standards represent the consensus of a considerable body of expertise.
- ☑ The Plan-Do-Check-Act (PDCA) process approach is already hugely successful in other long-standing and distinguished management systems such as ISO 9001, the standard for Quality Management, and ISO 14001, the standard for Environmental Management Systems.
- ☑ The PDCA is a robust model for implementing the principles set out in the 2002 OECD Guidelines.
- ☑ The PDCA process approach promises to achieve the sought after results more efficiently because the activities and the resources are managed as a process. This approach offers a number of key benefits such as improved, consistent, and predictable results; and the possibility to focus and prioritize improvement opportunities.
- ☑ The PDCA process approach helps us avoid the treating our "sore spots" with short-term fixes to symptoms, and instead look for long-term cures to the problem themselves.
- ☑ We need to identify related processes and manage them within a systems approach to realize both effectiveness and efficiency. No one department owns all the processes that contribute to the company's overall objective. Therefore, the systems approach will help us understand the interactions and consequences of addressing only a particular issue, and will achieve the integration and alignment that best brings about the desired results.
- ☑ The ISO/IEC 27001 ISMS standard specifies and tightly integrates the use of risk assessment and risk management methods into the PDCA process activities.
- ☑ The ISO/IEC 27002 Code of Practice is the preferred source for the selection of controls to mitigate risk. However, it is important to understand that not all the controls in the catalogue are obligatory.
- ☑ The ISO 27002 Code of Practice is a good starting point for implementing information security because the recommended controls represent common legislative requirements or widespread practices within the information security community.
- ☑ The ISO/IEC 27002 Code of Practice can function as the compliance catalogue so we can self-measure whether we have at least considered all of the controls.
- ☑ We still have freedom to manoeuvre, because the ISO/IEC simply requires that we select the controls we require based on our own unique security requirements so

long as we have reduced our risks to an acceptable level and we have documented this appropriately.

4

COMPARING SECURITY MANAGEMENT REQUIREMENTS

A MEANS OF COMPARISON

The Government of Canada has written its own standard, but this does not imply that they started from nothing. It is more likely that they "borrowed" from the information security community at large to construct a standard that is specifically "tuned" to their unique needs – perhaps by selecting the most common or best solutions for each set of controls. However, this line of thinking may leave them exposed without even knowing it. For example, these best security practices may have been pulled out of a prevailing standard without considering how they factored into the underlying process of that standard. Simply put, they have a long list of best practices, but the plan prescribing them may be disjointed making gaps and vulnerabilities difficult to pinpoint.

Of course, this inference is difficult to validate without suitable metrics – something that is proving very difficult for even the best organizations. Lacking suitable metrics, an alternative method is to compare the Government's standard against an appropriate benchmark, like a universally accepted standard.

The Auditor General has already pointed out that the Government of Canada lacks appropriate means to determine if gaps exists and they do not have an adequate basis to determine whether their current IT security practices are sufficient and appropriate. Therefore, Part III of this paper examines the standard which Canadian federal departments are obligated to implement (i.e., MITS) using the ISO standards as an appropriate benchmark of a comprehensive and effective information security program.

MAPPING MITS TO THE ISO/IEC 27001 ISMS REQUIREMENTS

Comparing requirements is simply a matching exercise, and not an exercise of judgement. The intent of this paper is not to make any inferences good or bad, right or wrong about the MITS standard. Rather, the intent is to allow Canadian federal departments to consider the comparisons and extrapolate their own conclusions.

Since the MITS standard allows for flexibility and interpretation, some departments will be further along and may indeed being doing more than the standard literally requires. On the other hand, some departments are struggling to meet the intent of specific MITS requirements. In either case, the comparisons below offer ideas for departments to consider towards improving their own IT security program.

ESTABLISH AND MANAGE (PLAN)

The key purpose of the "Plan" phase is to design and specify the objectives and processes necessary to deliver results in accordance with stakeholder requirements and organizational policies. In addition, this is where senior management demonstrates their commitment to information security by establishing its importance, providing effective and functioning governance at the highest level of the organization, establishing detailed organization and management responsibilities and accountabilities, allocating adequate resources to information security, and reporting for review the performance of the ISMS to executive level management.

Outputs of the Plan phase might include:

- ☑ Scope document describing the boundaries of the ISMS
- ☑ Information security policy documents
- ☑ Information and IT asset list requiring protection
- ☑ Risk assessment document
- ☑ List of controls and other risk prevention measures
- ☑ Risk treatment plan
- ☑ Statement of applicability
- ☑ Standards and procedural guidelines and templates
- ☑ Standards and procedures themselves
- ☑ Measures and metrics to gauge the effectiveness of implementation, monitoring, review, and revising the program

Table 2 summarizes the high-level requirements of ISO/IEC 27001 and shows where the MITS standard has comparable requirements.

Table 2. ISO/IEC 27001 "Plan" Requirements

ISO/IEC 27001 "Plan" Requirements	MITS Requirements
[4.2.1a] Define the scope and boundaries of the ISMS	
[4.2.1b] Define the ISMS policy	[10] Departmental IT security policy
[4.2.1c] Define the risk assessment approach	
[4.2.1d] Identify the risks	[12.3.2] Threat and risk assessment
[4.2.1e] Analyze and evaluate the risks	[12.3.2] Threat and Risk Assessment
[4.2.1f] Identify and evaluate options for the treatment of risks	[13] Graduated Safeguards [12.3.1] Graduation of Controls and Safeguards
[4.2.1g] Select control objectives and controls for the treatment of risks	[13] Graduated Safeguards
[4.2.1h] Obtain management approval of the proposed residual risks	
[4.2.1i] Obtain management authorization to implement and operate the ISMS	[9] Roles and Responsibilities
[4.2.1j] Prepare a statement of applicability	

Listed below are the major differences between the ISO/IEC 27001 requirements and the MITS requirements:

- 4.2.1a. MITS does not require departments to define the scope and boundaries of their IT security program. This is an important requirement intended to ensure that departments clearly identify any location, function, asset, or technology that they would like to exclude from a specific requirement for a valid reason. There may be the assumption that departments must apply the MITS standard across its entire department without exception.
- 4.2.1b. MITS does not require departments to establish the criteria against which risk will be evaluated.
- 4.2.1c. MITS states the requirement to continuously manage risks and even identifies some of the risk management tools, such as TRA, audits, business impact analysis, privacy impact assessments, self-assessments, security investigations, and vulnerability assessments. However, the MITS standard does not require departments to identify a risk assessment methodology, develop the criteria for accepting risk, or develop the acceptable risk levels. There may be an assumption

that departments are to use the methods developed or recommended by the Government of Canada Lead Security Agencies[25]

- ☒ 4.2.1f. MITS does not identify the policy or criteria for accepting risks, but does refer to the Government's Integrated Risk Management Framework, which outlines generic options for the treatment of risks.
- ☒ 4.2.1h. MITS does not specify what level of management can approve the residual risk.
- ☒ 4.2.1i. MITS directs that departments must designate individuals to perform specified functions related to IT security. Specifically, an IT Security Coordinator must be appointed to establish and manage the IT Security Program (i.e., ISMS) as part of a coordinated departmental security program. However, there is no specific direction that the IT Security Coordinator must obtain management authorization implement and operate the program. Is this assumed to happen?
- ☒ 4.2.1j. MITS does not direct departments to write a statement of applicability (SOA). The SOA is important for providing the reasons and justification for the selection or exclusion of any control objectives and controls. Justifying exclusions ensures that no controls have been inadvertently omitted.

IMPLEMENT AND OPERATE (DO)

The key purpose of the "Do" phase is to develop, implement, and operate the IT security program. Key activities include creating the mission and charter of the program; creating the necessary committees (i.e., steering committee, awareness committee, compliance committee, and policy committee); identifying and classifying the organization's assets that impinge on the program; and managing the operation and resources of the program. This is also when IT security management may identify issues that have not yet been addressed.

Outputs of the Do phase might include:

- ☑ Security handbook
- ☑ Business continuity management plan that includes BCP and DRP

[25] The GSP identifies and defines the roles and responsibilities of departments and agencies that play a lead role in information and IT security within the Government. For example, one of the responsibilities of the Communications Security Establishment (CSE) is to develop operational standards and technical documentation related to IT security in terms of system certification and accreditation, risk and vulnerability analysis, product evaluation, system and network security analysis. Another lead department, the Royal Canadian Mounted Police (RCMP) is responsible to provide advice to departments on the process of threat and risk assessments, and the conduct of IT system security reviews, inspections and audits.

- ☑ Awareness, training, and education materials and plans
- ☑ Operational description of the ISMS
- ☑ Incident management plan including incident reporting procedures and root cause analysis methods

Table 3 summarizes the high-level requirements of ISO/IEC 27001 and shows where the MITS standard has comparable requirements.

Table 3. ISO/IEC 27001 "Do" Requirements

ISO 27001 "Do" Requirements	MITS Requirements
[4.2.2a] Formulate a risk treatment plan	
[4.2.2b] Implement a risk treatment plan	
[4.2.2c] Implement controls	[12.3.2] Threat and risk assessment [13] Graduated safeguards
[4.2.2d] Assess control effectiveness	
[4.2.2e] Implement training and awareness program	[12.12] IT security awareness [12.13] IT security training
[4.2.2f] Manage operations of the ISMS	[9.1] IT Security Coordinator
[4.2.2g] Manage resources of the ISMS	[9.1] IT Security Coordinator
[4.2.2h] Implement the procedures and other controls capable of enabling prompt detection of and response to security incidents	[15] Active defence strategy [18.1] Incident response coordination [18.3] Incident response

Listed below are the major differences between the ISO/IEC 27001 requirements and the MITS requirements:

- ☒ 4.2.2a. MITS does not specify the requirement for a risk treatment plan. This is not to be confused with the mitigation controls identified in a TRA. The risk treatment plan is meant to be evidence of senior management commitment to the IT security program by identifying a management action plan, control objectives, resources, responsibilities, and priorities for managing risks.
- ☒ 4.2.2b. Following the above requirement, if there is no risk treatment plan, then there is no requirement to implement it.

- ☒ 4.2.2d. MITS does not define how to measure the effectiveness of the selected controls. This is important to allow management to determine how well controls achieve the planned control objectives.

MONITOR AND REVIEW (CHECK)

The key purpose of the "Check" phase is to monitor and review the program. This is when the organization determines whether the security activities delegated to people or implemented by technologies are performing as expected, typically done by self-assessment or external audits. As well, this phase provides the processes for management to ensure that the scope of the program remains adequate and improvements in the program are identified.

Outputs of the Check phase might include:

- ☑ Metrics and measurements for individual selected controls
- ☑ Updated list of residual risks
- ☑ Audit checklists
- ☑ Results from internal audits
- ☑ List of improvements for the ISMS

Table 4 summarizes the high-level requirements of ISO/IEC 27001 and shows where the MITS standard has comparable requirements.

Table 4. ISO/IEC 27001 "Check" Requirements

ISO 27001 "Check" Requirements	MITS Requirements
[4.2.3a] Execute monitoring and review procedures	[15] Active defence strategy [18.1] Incident response coordination [18.2] Incident identification and prioritization 18.3] Incident response
[4.2.3b] Undertake regular reviews of the effectiveness of the ISMS	[12.11.1] Self-assessment
[4.2.3c] Measure the effectiveness of controls	
[4.2.3d] Review risk assessments	[12.3.3] Certification and accreditation
[4.2.3e] Conduct internal ISMS audits at planned intervals	[12.11.2] Internal audit
[4.2.3f] Undertake a management review of the ISMS	
[4.2.3g] Update security plans to take into account the findings of monitoring and reviewing activities	[12.11.1] Self-assessment
[4.2.3h] Record actions and events that could have an impact on the effectiveness or performance of the ISMS	

Listed below are the major differences between the ISO/IEC 27001 requirements and the MITS requirements:

- 4.2.3b. MITS prescribes a management review for monitoring compliance with government and departmental policies and standards (a checklist approach), but does not address the need to review the scope of the IT security program or improvements to IT security processes. Furthermore, the self-assessment form prescribed by MITS has not been developed yet.
- 4.2.3c. MITS does not direct this requirement. Measurement and metrics are something that even the more advanced IT security programs struggle with.
- 4.2.3d. Departments must periodically review the accreditation of systems if the systems have changed significantly or if warranted due to changes in the risk environment. There is no specific requirement to review the risk assessment except as part of the review of the accreditation.
- 4.2.3f. MITS does not direct this requirement.
- 4.2.3g. Within MITS, monitoring and review activities do not prompt this requirement; but rather this requirement hinges on results of the annual self-assessment of the IT security program. If self-assessment is not completed, there is no mechanism to update IT security action plans.

- ☒ 4.2.3h. MITS does not direct this requirement.

MAINTAIN AND IMPROVE (ACT)

The key purpose of the "Act" phase is to maintain and improve the IT security program. The phase also allows for the identification of new business requirements and new risks.

Table 5 summarizes the high-level requirements of ISO/IEC 27001 and shows where the MITS standard has comparable requirements.

Table 5. ISO/IEC 27001 "Act" Requirements

ISO 27001 "Act" Requirements	MITS Requirements
[4.2.4a] Implement the identified improvements in the ISMS	[12.11] Departmental IT security assessment and audit
[4.2.4b] Take appropriate corrective and preventative actions	[15] Active defence strategy
[4.2.4c] Communicate the actions and improvements to all interested parties	
[4.2.4d] Ensure that improvements achieve their intended objectives	

Listed below are the major differences between the ISO/IEC 27001 requirements and the MITS requirements:

- ☒ 4.2.4a. MITS directs departments to actively monitor their management practices and controls and remedy deficiencies where necessary.
- ☒ 4.2.4c. MITS does not direct this requirement.
- ☒ 4.2.4d. MITS does not direct this requirement.

DOCUMENT, DOCUMENT, DOCUMENT

The ISO/IEC 27001 standard specifies additional requirements that cross the boundaries of the PDCA cycle. Such requirements include maintaining meticulous documentation that records management decisions, ensures that actions are traceable to management decisions and that recorded results are reproducible. This is important to demonstrate the links from control selection based upon a risk assessment and subsequently back to the security policy and objectives. As well, the organization must protect and control these documents and have defined procedures to accomplish this.

Additionally, the ISO/IEC 27001 standard spells out specific responsibilities for senior management, specific outcomes for its internal audits, and specific input and output documents required of the management review.

A process-oriented IT security program would expect to encounter these additional requirements since processes tend to change over time unless proper documentation keeps them on track. However, the MITS standard is clearly a checklist approach vice a process approach. Therefore, it is not surprising that these additional requirements are noticeably absent from the MITS standard.

OTHER GAP ANALYSIS MEANS

The gaps shown in Table 2 through Table 6 may not be completely indicative of the whole story. Departments need to consider that gaps can creep into their IT security program and hinder its success by means other than what might be obvious by doing a simple "checklist" comparison.

MANAGEMENT INDUCED GAPS

Management can cause a gap between strategy and execution through both action and inaction. Four main ways management causes this gap include failure to secure support for the plan, failure to communicate the strategy, failure to adhere to the plan, and failure to adapt to significant changes (Coveney, Canster, Hartlen, & King, 2003). The processes that management uses can also be a factor that introduces gaps. For example, a study of 23 U.S. Department of Defense (DoD) programs indicated that management processes for developing and deploying DoD systems were the primary contributors to poor process performance (Charette, Dwinner, & McGarry, 2004).

PROCESS INDUCED GAPS

Processes that we use to implement and monitor our IT security program are another means of introducing gaps. We still need to put into action programs that we have designed and specified. However, the way in which we perform these processes and the interfaces between the processes can lead to gaps (Coveney, Canster, Hartlen, & King, 2003). The study by Charette et al (2004) indicates that process performance shortfalls are the primary factor impeding a program to meets its objectives and technical performance requirements. The authors of this study observed that process performance shortfalls are a combination of different factors. For example, process performance is related to process adherence (i.e., the ability to adequately define and implement the process) and process capability (i.e., the effectiveness of the process). The authors' assessment was that process adherence shortfalls most often occur in areas of requirements definition, risk management, and technical change management. IT security "teams" should take this research to heart, for it indicates that they might experience trouble with defining, or implementing their processes.

To provide further clarity, Charette et al, described process adherence problems as two general types. A process may be poorly executed (i.e., meaning that the process is not implemented or performed effectively) or constrained (i.e., meaning that it is not fully implemented or executed because it is not sufficiently supported or funded). For IT security, these constrained processes typically result from trading off IT security requirements against "higher-priority" organizational requirements.

TECHNOLOGY INDUCED GAPS

The final way that can cause gaps involves the traditional tools that we use to support the IT security program, such as software tools for planning, budgeting, forecasting, and reporting. Fragmented systems and misplaced dependence on enterprise resource tools can also introduce gaps (Coveney, Canster, Hartlen, & King, 2003). IT security staffs need to include these tools as inputs into the process to ensure they are accounted for.

SUMMARY OF KEY POINTS

- ☑ The "Plan" phase is where we design and specify our objectives and processes. This is where senior management demonstrates their commitment to information security.
- ☑ The "Do" phase is where we develop, implement, and operate the IT security program. This is where we may identify issues that have not yet been addressed.
- ☑ The "Check" phase is where we monitor and review the program. This is when we determine whether the security activities delegated to people or implemented by technologies are performing as expected.
- ☑ The "Check" phase provides the processes for senior management to ensure that the scope of the program remains adequate and improvements in the program are identified.
- ☑ The "Act" phase is where we maintain and improve the IT security program. This phase allows for the identification of new business requirements and new risks.
- ☑ The ISO/IEC 27001 ISMS requires us to maintain meticulous documentation that records management decisions, ensures that actions are traceable to management decisions and that recorded results are reproducible.
- ☑ Departments need to consider that gaps can creep into their IT security program and hinder their success by means other than what might be obvious from doing a "checklist" gap analysis.

5

STEPS-TO-SUCCESS

"If your business isn't moving fast enough, consider the turtle...It can't move at all if it doesn't stick its neck out" - Anonymous

There are many publications, consultants, and other subject matter experts offering strategies to close the gaps. This paper does not claim to provide the best solution tuned specifically to Canadian federal government departments' needs. Rather the steps-to-success presented here are simply one way to approach closing the gaps. These steps represent a collage of the seminal thinking by many so-called experts[26].

GETTING THERE IN NINE NOT-SO-EASY STEPS

"The basic need for a process is simple – to keep the amount of spur of the moment decisions to a minimum." - Anonymous

STEP 1: GET "VISIBLE" EXECUTIVE MANAGEMENT COMMITMENT

Even if you were the CISO, relying on your own sense of responsibility and your initiative to drive improvements in your information security program would be a mistake. Visible support and commitment from executive management is critical. While most experts agree that this will not guarantee success, lack of it will guarantee failure. Do not underestimate this step. Top management support is the number one issue facing information security professionals today, ahead of user awareness training and education (Knapp, Marshall, Rainer, & Morrow, 2006).

Section 5.1 of the ISO/IEC 27001 standard lists a number of ways that senior management can show their commitment. Some quick wins for government departments might include the following:

[26] Some of the ideas presented in this section of this paper were inspired by Robert A. Neiman's book "Execution Plain and Simple: Twelve Steps to Achieving Any Goal On Time And On Budget" 2004. New York: McGraw-Hill Companies Inc.

- ☑ Decide the criteria for accepting risk and the acceptable levels of risk. Ensure this is written into policy and communicated to all relevant stakeholders.
- ☑ Conduct a management review of the IT security program.
- ☑ Insist on regular status reports indicating progress towards improvement goals.
- ☑ Endorse the improvement plan and personally address the kick-off meeting. This is important to ensure that the entire organization recognizes the need for change and to create buy-in.
- ☑ Assign responsibility to make sure that is "actually happens" to a C-level executive and ensure that it is not delegated downwards. The C-level executive is necessary to enable cross-boundary motivation and achieve real transformation.
- ☑ Approve and sign a Statement of Applicability (SOA) to link an executive level decision to the risk concerns.

STEP 2: DEFINE THE ASSIGNMENT IN WRITING

An assignment in writing is your official charge to move forward. It confirms that the task of improving your IT security program is real. However, to be perceived as a true and honest requirement, the official assignment must come from the highest level of the organization that is accountable for IT security. Do not expect executive management to write this assignment. You need to construct it so the following implicit and implied tasks and motivational messages are covered:

- ☑ Know your status quo.
- ☑ Define the problem in terms of processes and show, in an unambiguous way, how processes work. Drive home the message of doing things consistently.
- ☑ Reinforce the message that this is not just a paperwork exercise. Although a lot of documentation will be produced, the benefits of the resulting thought processes, awareness, and informed-choice decision making far outweigh the resulting documentation.
- ☑ Decide early which processes need to be standardized organization-wide and which processes need to remain flexible to meet the unique needs of lower-level operations. Identify the potential constraints or bottlenecks.
- ☑ Assign authority and responsibility for the improvement of organization-wide processes to designated process owners. Process owners must form appropriate cross-functional teams, monitor progress, and publish results to other process owners where an interface occurs.
- ☑ Establish a senior steering committee to resolve issues at the process interface points.
- ☑ Creating a significant improvement will require a radical shift – not just fine-tuning.

STEP 3: ORGANIZE A CORE TEAM AND CREATE A STRATEGY

Be selective when you make choices of who should be the core team members. Without dwelling on Management 101, you should consider such qualities as,

competence, representative, influence, availability, loyalty, and candour when you select your team.

As for strategy, you do not need to be firm at this point. A simple story about what needs to be done will provide enough of a framework to proceed. At most, the strategy should fit on one page. Longer strategy documents do not necessarily indicate that you have done more thinking about it and could even become constraining. The one-page strategy is more easily understood and explainable in plain language to the people who will do the work. Some ideas for selecting your core team and writing your strategy are:

- ☑ Select the right people with the right skills and a continuous improvement mindset.
- ☑ Show the similarities of your improvement plan to a credible and already successful strategy, such as ISO 9001, ISO 14001, and now ISO 27001.
- ☑ Show how is will be easier to collect metrics to analyze and produce feedback for continuous improvement.
- ☑ Focus on the problems that are causing the most pain and target these for immediate improvement efforts. Accept that getting it perfect is not the aim and that adjustments may be necessary later on after you have implemented the solution.
- ☑ Focus on how the processes fit together (in a system). Recognize that the principle of sub-optimization[27] will not lead to better output overall.
- ☑ Do not hype and set expectations for instant results. Process improvement is hard and not everything you plan can be realistically achieved. Recognize that you will not have the resources to do a complete one-shot overhaul. Therefore, you need to plan for a series of agreed-upon process improvement efforts (both strategic and tactical), including prioritization, timeframes, and resources. The smaller and more focused the processes, the better you will be able to steal time away from daily tasks and focus on accomplishing improvements[28].

STEP 4: GET INPUT AND SUPPORT FROM KEY PLAYERS

Other people will have an opinion about your IT security improvement ideas. Do not forget about them. Take this opportunity to get help from them or to get real

[27] The principle of sub-optimization asserts that optimizing each process independently, in general, will not lead to an increased optimization for the overall system. The act of sub-process improvement frequently causes the exact opposite of the indented outcome (i.e. the whole is less than the sum of its parts). [Mark Lefowitcz – Why Process Improvements Fail]

[28] From Enterprise Computing Institute: Top 5 Reasons Why ITIL Implementations Don't Happen by the Books.

problems out of the way before you get too far down your path. They may be able to identify other key players affected by your initiatives or give you a good indication of the reaction you might receive from others. This will also help you generate broader interest in your initiative. If necessary, this is the point where you can adjust your strategy. Some tips and ideas to help you here are:

- ☑ Initialize process improvement goals through peer collaboration groups and benchmarking.
- ☑ Be wary that your process improvements efforts do not trigger increased internal competition for scarce operating resources, which may in turn lead to personal, functional unit or organization cultural conflicts.
- ☑ Look at the processes from the clients' perspective.
- ☑ Do not underestimate the importance of being able to call for external competence when needed - access to external competence is a critical success factor.

STEP 5: CREATE MOMENTUM

This is the time to "launch" your initiative. Your launch event defines the transition from strategy to action. It takes special effort to get people's attention and to do something new so assemble the highest-ranking people you can in one location and prove to them you are on the right path. Here are some ideas:

- ☑ Demonstrate how following a credible process approach will make your IT security program and the decisions flowing from it, more defensible. This may be incredibly valuable and important when dealing with your interconnected "partners."
- ☑ Demonstrate how the desired improvements will enhance the perception and image of your IT security program. This is important so your clients see your program as an enabler and not an inhibitor to their day-to-day work.
- ☑ Make immediate implementation of some quick wins to prove commitment to making improvements.
- ☑ Show how focusing on processes can reduce the amount of redundant work in the organization.
- ☑ Invest in powerful process improvement tools for your team. This will minimize the learning curve and reinforce standardization.

STEP 6: PRESENT A ROADMAP

This is where you spell out the specific tasks in writing to your teams. Your teams need to know all the gritty details and the written work plan is the principal tool for guiding their actions and managing the execution of their tasks. Consider the following tips:

- ☑ Measure current performance and identify root causes of poor performance. Do not try to measure everything. Focus your measurements on those outputs required for

the next stage in the system and those that contribute to client satisfaction. These should be your key performance indicators (KPI).

- ☑ Define the process first, and then focus on methods you can use to execute it.
- ☑ Map and understand dependencies between processes.
- ☑ Strike an appropriate balance between strategic improvement efforts and tactical improvement efforts. Tactical teams will want to focus on day-to-day processes like change control and incident management. However, strategic teams will want to focus on resource management and service delivery levels. A heavy strategic hand will alienate the tactical teams and they may see the effort as just another management thing being pushed on them that does not improve what they are doing. A heavy tactical hand will alienate the strategist, and then your improvement plan comes to a grinding halt.
- ☑ Recognize that the "keep it up and running" attitude (to meet tough availability requirements) will not disappear. This means that your day-to-day work will not diminish and will always triumph over your process improvement efforts.
- ☑ Do not attempt to measure everything or add all the "bells and whistles." Simple is easy to understand; simple is easy to follow. The objective is not to have a perfect plan, but to enable effective action to deal with real day-to-day problems.
- ☑ Start with a general outline your long-term plan showing the major pieces of work and expected timelines. Then create and work from 30-60-90 day plans within the longer framework.

STEP 7: ENGAGE THE ORGANIZATION

Do not let your plan stall. You need to fuel longer plans, especially ones that might take multiple fiscal budgets to accomplish. Try these tactics:

- ☑ Use success stories to celebrate and reinforce your improvement initiatives.
- ☑ Celebrate to wake dormant people, turn wafflers and doubters into advocates and sceptics into supporters.
- ☑ Acknowledge and celebrate quick wins when they occur.

STEP 8: FOLLOW UP

Keep your initiative moving and hold your teams accountable. Here are some ideas:

- ☑ Use rigorous standardization to reduce variation in processes and create predictable outcomes. Minimize variation without oppressing innovation, creativity, and flexibility.
- ☑ Conduct one-on-one reviews with the people doing the assignments.
- ☑ Conduct group progress reviews.
- ☑ Have executive management do regular personal site visits.

- ☑ Train your people how to work with the improved processes. This is more than just publishing the procedure and directing compliance with it.

STEP 9: LEARN FROM EXPERIENCE AND SHARE WHAT YOU LEARN

Track the knowledge and experience you gain as you proceed, and do not be shy about sharing this with the rest of the organization. Keep in mind that lessons are not learned until behaviour is changed.

- ☑ Baseline the process.
- ☑ Imitate others you are already doing the process well.
- ☑ Publically announce your lessons learned, especially share what does not work so that other can avoid similar pitfalls.

6

EPILOGUE

"Nothing is more rewarding that to watch someone who says it can't be done get interrupted by someone who is actually doing it" – John M. Capozzi

A MILLION REASONS NOT TO

It is normal for some organizations (especially government) to develop their own IT security standards rather than adopting a standard that they had no hand in writing. This is what the Canadian Government has done with their MITS. Since these standards are imposed downward, it is just as normal for government departments to exclude consideration for other standards or approaches. This is understandable since departments already have a standard they are obligated to implement, and substantiating plans and resources to meet this standard is straightforward. Given this situation, self-justifying reasons not to pursue other standards or approaches are plentiful - some valid, some not so valid - but all convincing nonetheless. Here are just some of them.

- "We are different." We have our own unique standard that was specifically crafted to meet our needs. Why would we need anything else?
- "Senior management will simply not give us any more resources." It is much more difficult to persuade top-level management for resources to implement an additional voluntary standard even for those seasoned in writing business cases.
- "Only parts of that standard fit our needs." We do not agree with everything in the standard.
- "We do not have any influence over changes to the standard." The standard is continually evolving, so our unique needs might be dropped during the updates and changes.
- "We will be locked into continual updates." Once we adopt the standard, will be obligated to implement the updates, even if we do not feel that it adds any real value for us.
- "We do not need that much protection." The standard entails a much stricter application of controls than what we currently practice.
- "It does not allow us the flexibility we need." The standard is too prescriptive.
- "We can barely keep up with our current workload and you are asking us to take on more." We are suffering from staffing and funding crunches that frankly, make it difficult to keep up with our current workload.

LAST WORDS

The decision to implement standards, beyond what we are already obligated to implement, has to be a strategic one not a tactical one – and the decision has to come from the highest level of management accountable for information security. The work to get there will be hard, perhaps long, and most probably frustrating.

Finally, the communication plan has to be organization-wide. This cannot be played out as just another management "fad" that has to be endured until it goes away, or even worse, an IT Department initiative! Ideally, this initiative should be placed where it has a real chance to achieve organizational alignment. It should be led by a C-level executive who is independent of the IT organization with a cross-functional team as a supporting cast. Once independence is achieved, the perceptions, stereotypes, and stigmas generally attributed to IT security improvement may diminish.

References

Arnason, Sigurjon Thor., & Willett, Keith D. (2008). *How to Achieve 27001 Certification: An Example of Applied Compliance Management*. New York. Auerbach Publications.

Auditor General of Canada. (2002). *Information Technology Security* (Report of the Auditor General of Canada to the House of Commons, p. Chapter 3). Ottawa, Canada: Minister of Public Works and Government Services Canada.

Auditor General of Canada. (February 2005). *Information Technology Security* (Follow-Up Report of the Auditor General of Canada, p. Chapter 1). Ottawa, Canada.

BSI British Standards. (Ed.). (2001, November). *BS7799-2 Information security management part 2 - specification for information security management systems.* (Available from BSI Group, www.bsi-global.com)

BSI British Standards. (Ed.). (2001, November). (Available from BSI Group, www.bsi-global.com)

Caralli, R. A. (2006). *Sustaining Operational Resiliency: A Process Improvement Approach to Security Management* (TECHNICAL NOTE CMU/SEI-2006-TN-009). United States: Carnegie Mellon University. Retrieved Auguest 10, 2008, from Software Engineering Institute - Carnegie Mellon Web site: http://www.sei.cmu.edu/publications/documents/06.reports/06tn009.html

Charette, Dwinnell, L. M., & McGarry, J. (2004). Understanding the Roots of Process Performance Failure. *Cross Talk the Journal of Defense Software Engineering, August, pages* 18-22.

Chien Te-King, Lai Wen-Ling, Hsu Wei-Chen, & Wang Mei-Fang. (2007, July 11-13). *A Study of ISMS Implementation Road Map*. Research Paper presented at the International Conference on Business and Information, Tokyo.

Coveney, G., Canster, D., Hartlen, B., & King, D. (2003). *The Strategy Gap*. Hoboken, New Jersey: John Wiley & Sons.

Curt Fleming. (2002). Understanding the Process Approach of ISO 9000:2000. *Medical Device & Diagnostic Industry, October*. Retrieved July 03, 2008, from Medical Device Link Web site: http://www.devicelink.com/mddi/archive/02/10/001.html

Cyber Security Strategy Committee. (2008). *Cyber Security Strategy* [Electronic version]. Tallin, Estonia: Ministry of Defence.

de Bruin, T., & Rosemann, M. (2006, 6-8 December). *Towards Understanding Strategic Alignment of Business Process Management*. Conference Papers and Proceedings presented at the 17th Australasian Conference on Information Systems, Adelaide, Australia.

Douglas G. Timmins, Assistant Auditor General. (2002, 12 May). *Information Technology Secuirty*. Opening Statement to the Standing Committee on Public Accounts presented at the House of Commons Canada, Ottawa, Canada.

Douglas G. Timmins, Assistant Auditor General. (2005, 23 March). *Information Technology Security*. Opening Statement to the Standing Committee on Public Accounts presented at the Chapter 1 - February 2005 Report of the Auditor General of Canada, Ottawa, Canada.

Federal Trade Commission. (2002). Standards for safeguarding consumer information: final rule. In *16 CFR Part 314* (RIN 3084 AA87). Washington, DC: Federal Register Part VII.

Gillian Shaw. (2008, November 25). Canadian cybercrime inaction called an embarrassment. *Vancouver Sun*. Conner, B., Noonan, T., & Holleyman, R. W. (2003). *Information security governance: toward a framework for action*. Retrieved June 10, 2005, from The Business Software Alliance Web site: http://www.bsa.org

INCITS. (2006). ISO/IEC 27001-2005 Information technology - security techniques - information security management systems - requirements. In *American National Standard*. New York: American National Standards Institute.

ISO/IEC. International Organization for Standardization, & the International Electromechanical Commission. (2004, May 13). *Introduction and support package guidance on the concept and use of the process approach for management systems* (Document: ISO/TC 176/SC 2?N544R(r)). Author. Retrieved July 03, 2008, from ISO Web site: http://www.iso.org/iso/iso_catelogue/management_standards

ISO/IEC. International Organization for Standardization, & the International Electromechanical Commission. (2005). *Code of practice for information security management* (ISO/IEC 17799). New York: American National Standards Institute.

ISACA. (2009). *An Introduction to the Business Model for Information Security*. Rolling Meadows, IL. Retrieved March 03, 2009, from ISACA Web site: www.isaca.org/security

IT Governance Institute. (2004). *IT control objectives for Sarbanes-Oxley: the importance of IT in the design, implementation and sustainability of internal control over disclosure and financial reporting*. Retrieved February 1, 2006, from IT Governance Institute Web site: http://www.itgi.org

Knapp, K.J., Marshall, T.E., Rainer, R.K., & Morrow, D.W. (2006). The top information security issues facing organizations: What can Government do to help? *Information Security and Risk Management, September/October*, 51-58.

Neiman, Robert A. (2004). *Execution Plain and Simple: Twelve Steps to Achieving Any Goal On Time And On Budget*. New York: McGraw-Hill Companies Inc.

Organisation for Economic Co-operation, & Development (OECD). (2002). *Guidelines for the security of information systems and networks: towards a culture of security*. (Original work published 1992) Retrieved February 12, 2006, from OECD Web site: http://www.oecd.org

Richard A. Caralli. (2006). *Sustaining Operational Resiliency: A Process Improvement Approach to Security Management* (Technical Note CMU/SEI-2006-TN-009). Pittsburgh, PA: Software Engineering Institute - Carnegie Mellon University.

Sheila Fraser, Auditor General of Canada. (2005, 16 February). *February 2005 Status Report of the Auditor General of Canada*. Opening Statement to the Standing Committee on Public Accounts, Ottawa, Canada.

Ted Humphreys. (2006). State-of-the-art information security management systems with ISO/IEC 27001:2005. *ISO Management Systems, January-February*, 15-18.

Treasury Board of Canada Secretariat. (2004). *Operational Security Standard: Management of Information Technology Security (MITS)*. Ottawa, Canada: Government of Canada.

Wim P.M. Vanhaverbeke & Huub M.P. Torremans. (1998, July 9-11). *Organizational Structure in Process-Based Organizations*. Research Paper presented at the 14th EGOS Conference, Maastricht, Netherlands.

APPENDIX A

COMPARING THE CATALOGUES OF SAFEGUARDS

"If you want the rainbow, you gotta put up with the rain"

MAPPING MITS TO THE ISO/IEC 27002 CODE OF PRACTICE

As noted earlier, the ISO/IEC 27002 standard serves as a catalogue of control objectives and controls that an organization can select from for the treatment of identified risks. While not an exhaustive list, this standard does provide a considerable shopping list of best security practices within a single document. However, the Government of Canada has divided its operational and technical level standards among multiple documents making a comparison of all its standards with ISO/IEC 27002 beyond the scope of this paper and making a valid gap analysis impractical. Nevertheless, the operational and technical controls included as part of the MITS standard are mapped here purely to show how they would fit into the ISO/IEC structure.

Table 6 summarizes the high-level requirements of ISO/IEC 27002 and shows where the MITS standard has included comparable requirements. This table provides a suitable mechanism for federal departments to map their remaining operational and technical standards and determine their own gaps. The remaining standards to which MITS refers to, but which are not mapped here, are:

- ☒ Intrusion detection
- ☒ Incident management
- ☒ Security training and awareness
- ☒ Security in contracting management
- ☒ Identification and categorization of assets
- ☒ Threat and risk assessment
- ☒ Investigations and sanctions
- ☒ Personnel security and security screening
- ☒ Department security program
- ☒ Protection of employees

- ☒ Security outside Canada
- ☒ Sharing of information
- ☒ Physical Security
- ☒ Business Continuity Plan[29]

Remember, not all of the controls in the ISO/IEC 27002 are necessary because these controls are intended to be applied based on the risk assessment of the organization.

Finally, government departments consider that the MITS standard prescribes additional safeguards that do not fit into one of the Table 6 grouping. These safeguards are likely unique to your departmental requirements and therefore, should not be discounted for their importance.

[29] List of standards that the Government of Canada is proposing and/or exists in DRAFT form is from the Auditor General of Canada (2005)

Table 6. ISO/IEC 27002 Control Objectives and Controls

ISO/IEC 27002 – Control Sets, Control Objectives and Controls	MITS Comparable Safeguards
[5] SECURITY POLICY	
[5.1] Information Security Policy	
[5.1.1] Information security policy document	[10] Departmental IT security policy; and [9.2] Senior management
[5.1.2] Review of the information security policy	[10] Departmental IT security policy
[6] ORGANIZATION OF INFORMATION SECURITY	
[6.1] Internal Organization	
[6.1.1] Management commitment to information security	[9.2] Senior management
[6.1.2] Information security co-ordination	[9.1] IT security coordinator
[6.1.3] Allocation of information security responsibilities	[9] Roles and responsibilities, including sub-parts [9.1] to [9.10]
[6.1.4] Authorization process for information processing facilities	[12.3.3] Certification and accreditation
[6.1.5] Confidentiality agreements	
[6.1.6] Contact with authorities	
[6.1.7] Contact with special interest groups	
[6.1.8] Independent review of information security	
[6.2] External Parties	
[6.2.1] Identification of risks related to external parties	
[6.2.2] Addressing security when dealing with customers	
[6.2.3] Addressing security in third party agreements	[12.7] Contracting

ISO/IEC 27002 – Control Sets, Control Objectives and Controls	MITS Comparable Safeguards
[7] ASSET MANAGEMENT	
[7.1] Responsibility for Assets	
[7.1.1] Inventory of assets	[12.2] Identification and categorization of information and IT assets. Refers to another standard *Operational Security Standard for the Identification and Categorization of Assets*
[7.1.2] Ownership of assets	
[7.1.3] Acceptable use of assets	
[7.2] Information Classification	
[7.2.1] Classification guidelines	
[7.2.2] Information labelling and handling	
[8] HUMAN RESOURCE SECURITY	
[8.1] Human Resources Security	
[8.1.1] Roles and responsibilities	[9] Roles and responsibilities
[8.1.2] Screening	[16.3] Personnel security in the IT security environment. Refers to another standard *Operational Security Standard on Security Screening*
[8.1.3] Terms and conditions of employment	
[8.2] During Employment	
[8.2.1] Management responsibilities	
[8.2.2] Information security awareness, education and training	[12.12] IT security awareness; and [12.13] IT security training
[8.2.3] Disciplinary process	[12.9] Sanctions. Refers to other standards *Operational Security Standards on Sanctions;* and *Treasury Board Guidelines for Discipline*

ISO/IEC 27002 – Control Sets, Control Objectives and Controls	MITS Comparable Safeguards
[8.3] Transition or Change of Employment	
[8.3.1] Termination responsibilities	
[8.3.2] Return of assets	
[8.3.3] Removal of access rights	[16.4.3] Authorization and access control
[9] PHYSICAL AND ENVIRONMENT SECURITY	
[9.1] Secure Areas	
[9.1.1] Physical security perimeter	[16.1] Physical security within the IT security environment. Refers to another standard *Operational Security Standard on Physical Security*
[9.1.2] Physical entry controls	
[9.1.3] Securing offices, rooms and facilities	
[9.1.4] Protecting against external and environment threats	
[9.1.5] Working in secure areas	
[9.1.6] Public access, delivery and loading areas	
[9.2] Equipment Security	
[9.2.1] Equipment siting and protection	
[9.2.2] Supporting utilities	
[9.2.3] Cabling security	
[9.2.4] Equipment maintenance	
[9.2.5] Security of equipment off-premises	
[9.2.6] Secure disposal or re-use of equipment	
[9.2.7] Removal of property	

ISO/IEC 27002 – Control Sets, Control Objectives and Controls	MITS Comparable Safeguards
[10] COMMUNICATIONS AND OPERATIONS SECURITY	
[10.1] Operational Procedures and Responsibilities	
[10.1.1] Documented operating procedures	
[10.1.2] Change management	[14.1] Configuration management and change control
[10.1.3] Segregation of duties	[12.6] Segregation of responsibilities
[10.1.4] Separation of development, test and operational facilities	
[10.2] Third Party Service Delivery Management	
[10.2.1] Service delivery	
[10.2.2] Monitoring and review of third party services	
[10.2.3] Managing changes to third party services	
[10.3] System Planning and Acceptance	
[10.3.1] Capacity management	[14.3] Capacity planning
[10.3.2] System acceptance	[12.3.3] Certification and accreditation
[10.4] Protection Against Malicious And Mobile Code	
[10.4.1] Controls against malicious code	[16.4.12] Malicious code
[10.4.2] Controls against mobile code	[16.4.11] Software integrity and security configuration
[10.5] Back-up	
[10.5.1] Information back-up	[18.5] Recovery
[10.6] Network Security Management	

ISO/IEC 27002 – Control Sets, Control Objectives and Controls	MITS Comparable Safeguards
[10.6.1] Network controls	[16.4.6] Network security and perimeter defence. Recommends use of another guide *Baseline Security Requirements for IT Security Zones*
[10.6.2] Security of network services	
[10.7] Media Handling	
[10.7.1] Management of removable media	
[10.7.2] Disposal of media	[16.2] Storage, disposal, and destruction of IT media
[10.7.3] Information handling procedures	
[10.7.4] Security of system documentation	
[10.8] Exchange of Information	
[10.8.1] Information exchange policies and procedures	[12.10] Sharing and exchange of information and IT assets
[10.8.2] Exchange agreements	[12.10] Sharing and exchange of information and IT assets
[10.8.3] Physical media in transit	
[10.8.4] Electronic messaging	
[10.8.5] Business information systems	
[10.9] Electronic Commerce Services	
[10.9.1] Electronic commerce	
[10.9.2] On-line transactions	
[10.9.3] Publicly available information	
[10.10] Monitoring	
[10.10.1] Audit logging	[9.7] IT operational personnel ; and [17] Detection
[10.10.2] Monitoring system use	[9.7] IT operational personnel

ISO/IEC 27002 – Control Sets, Control Objectives and Controls	MITS Comparable Safeguards
[10.10.3] Protection of log information	
[10.10.4] Administrator and operator logs	
[10.10.5] Fault logging	
[10.10.6] Clock synchronization	[14.4] System support services
[11] ACCESS CONTROL	
[11.1] Business Requirements for Access Control	
[11.1.1] Access control policy	[16.4.3] Authorization and access control
[11.2] User Access Management	
[11.2.1] User registration	
[11.2.2] Privilege management	[16.4.3] Authorization and access control
[11.2.3] User password management	
[11.2.4] Review of user access rights	[16.4.3] Authorization and access control
[11.3] User Responsibilities	
[11.3.1] Password use	
[11.3.2] Unattended user equipment	
[11.3.3] Clear desk and clear screen policy	
[11.4] Network Access Control	
[11.4.1] Policy on use of network services	
[11.4.2] User authentication for external connections	
[11.4.3] Equipment identification in networks	

ISO/IEC 27002 – Control Sets, Control Objectives and Controls	MITS Comparable Safeguards
[11.4.4] Remote diagnostic and configuration port protection	
[11.4.5] Segregation in networks	[16.4.6] Network security and perimeter defence
[11.4.6] Network connection controls	
[11.4.7] Network routing control	
[11.5] Operating System Access Control	
[11.5.1] Secure log-on procedure	
[11.5.2] User identification and authentication	[16.4.2] Identification and authorization
[11.5.3] Password management system	
[11.5.4] Use of system utilities	
[11.5.5] Session time-out	
[11.5.6] Limitation of connection time	
[11.6] Application and Information Access Control	
[11.6.1] Information access restrictions	
[11.6.2] Sensitive system isolation	
[11.7] Mobile Computing and Teleworking	
[11.7.1] Mobile computing and communications	[16.4.7] Mobile computing and Teleworking
[11.7.2] Teleworking	[16.4.7] Mobile computing and Teleworking
[12] INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE	
[12.1] Security Requirements of Information Systems	
[12.1.1] Security requirements analysis and specification	[11] IT security resources for projects [12.1] Security in the system development lifecycle

ISO/IEC 27002 – Control Sets, Control Objectives and Controls	MITS Comparable Safeguards
[12.2] Correct Processing in Applications	
[12.2.1] Input data validation	
[12.2.2] Control of internal processing	
[12.2.3] Message integrity	
[12.2.4] Output data validation	
[12.3] Cryptographic Controls	
[12.3.1] Policy on use of cryptographic controls	[16.4.4] Cryptography
[12.3.2] Key management	[9.9] COMSEC custodian
[12.4] Security of System Files	
[12.4.1] Control of operational software	[16.4.11] Software integrity and security configuration
[12.4.2] Protection of system test data	
[12.4.3] Access control to program source code	
[12.5] Security in Development and Support Processing	
[12.5.1] Change control procedures	
[12.5.2] Technical review of applications after operating system changes	
[12.5.3] Restrictions on changes to software packages	
[12.5.4] Information leakage	
[12.5.5] Outsourced software development	
[12.6] Technical Vulnerability Management	

ISO/IEC 27002 – Control Sets, Control Objectives and Controls	MITS Comparable Safeguards
[12.6.1] Control of technical vulnerabilities	[12.5] Vulnerability management [12.5.1] Vulnerability assessments [12.5.2] Patch management
[13] INFORMATION SECURITY INCIDENT MANAGEMENT **[13.1] Reporting Information Security Events and Weaknesses**	
[13.1.1] Reporting information security events [13.1.2] Reporting security weaknesses	[14.2] Problem reporting/help desk
[13.2] Management of Information Security Incidents and Improvements	
[13.2.1] Responsibilities and procedures	[12.4] Incident management [15] Active defence strategy[30] [17] Detection
[13.2.2] Learning from information security incidents [13.2.3] Collection of evidence	
[14] BUSINESS CONTINUITY MANAGEMENT **[14.1] Information Security Aspects of Business Continuity Management**	
[14.1.1] Including information security in the business continuity management process	[12.8] Continuity planning. Refers to another standard ***Business Continuity Planning Program Operational Security Standard***

[30] An active defence strategy includes four lines of defence: (1) prevention, (2) detection, (3) response, and (4) recovery.

ISO/IEC 27002 – Control Sets, Control Objectives and Controls	MITS Comparable Safeguards
[14.1.2] Business continuity and risk assessment [14.1.3] Developing and implementing continuity plans including information security [14.1.4] Business continuity planning framework [14.1.5] Testing, maintaining and re-assessing business continuity plans	
[15] COMPLIANCE [15.1] Compliance and Legal Requirements	
[15.1.1] Identification of applicable legislation [15.1.2] Intellectual property rights (IPR) [15.1.3] Protection of organizational records [15.1.4] Data protection and privacy of personal information [15.1.5] Prevention of misuse of information processing facilities [15.1.6] Regulation of cryptographic controls	
[15.2] Compliance with Security Policies and Standards, and Technical Compliance	
[15.2.1] Compliance with security policies and standards [15.2.2] Technical compliance checking	[9.1] IT security coordinator; and [12.11.1] Self-assessment
[15.3] Information Systems Audit Considerations	
[15.3.1] Information system audit controls	[12.11.2] Internal audit

ISO/IEC 27002 – Control Sets, Control Objectives and Controls	MITS Comparable Safeguards
[15.3.2] Protection of information systems and tools	