Microsoft MITS Compliance Planning Guide

Contents

Introduction

The Management of Information Technology Security (MITS) standard is an Operational Security Standard promulgated by Treasury Board Secretariat (TBS) that identifies a minimum baseline standard of care for IT Security within the Government of Canada (GoC). All GoC departments and agencies must comply with MITS by December 2006. This *Microsoft MITS Compliance Planning Guide* is designed to help IT managers and other key stakeholders within the GoC understand how Microsoft products and services can help them comply with many of the mandatory requirements identified in the MITS standard.

It should be noted that this guide should serve only as a complementary resource to assist in meeting the mandatory requirements identified within MITS. It should only be used as part of a comprehensive approach to information security as some of the requirements stated under MITS are outside the scope of vendor products and services. However, Microsoft customers should find that this guide will serve as a useful tool to help identify how Microsoft's products and services can be employed to meet applicable mandatory requirements identified within the MITS standard.

Approach

While compliance with MITS is currently in the forefront with the GoC and the primary focus of this guide, it is recognized that the MITS standard is not the only source of guidance that GoC departments and agencies must take into consideration. In fact, GoC departments and agencies must also adhere to other sources, including additional GoC policies and guidelines as well as applicable legislation. In addition, non-GoC organizations such as provincial and municipal governments as well as private industry also have a variety of regulations and guidelines that apply to them. It is therefore prudent to include a generic approach to compliance that is not MITS specific so that other sources of compliance can be considered, and non-GoC entities can take advantage of portions of this guide.

This leads to the approach illustrated in Figure 1. Specifically, we define a generic framework based on 20 technology solution categories that can be used to help IT managers and other key stakeholders understand what needs to be taken into consideration from a generic perspective. This generic framework can then be used to help map IT compliance requirements against the identified technical categories. We then map major sections from the MITS standard against the 20 technology categories in order to identify which technology categories are applicable to a given section within the MITS standard. Finally, we provide a detailed MITS compliance matrix (Annex A) that identifies specific Microsoft products and services that can help GoC departments and agencies comply with over 100 mandatory MITS requirements.

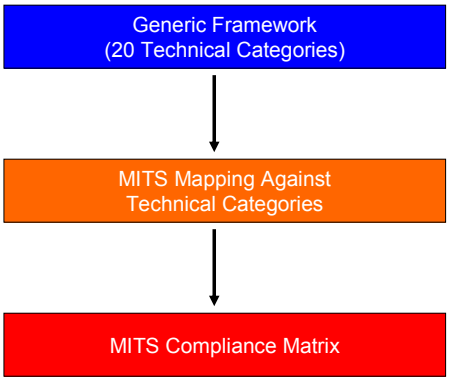

Figure 1: Approach

Thus, the intent of this guide is to assist IT managers and other key stakeholders achieve two primary goals:

- First, to help IT managers and other key stakeholders better understand *what* they need to know to address their regulatory compliance requirements. To achieve this, the guide provides a generic framework-based approach to compliance.
- Second, to help IT managers and other key stakeholders understand *how* they can address many of the mandatory MITS requirements that apply to their organization. To achieve this, the guide provides information about solutions that you can use to address the vast majority of the mandatory MITS requirements.

Who Should Read This Document

The audience for this guide includes IT managers who serve their organizations in the following positions:

- **Chief Information Officers (CIOs)** who are concerned with the deployment and operation of systems and IT-related processes.
- **Chief Information Security Officers (CISOs)** who are concerned with the overall information security program and compliance with information security policies.
- **Chief Privacy Officers (CPOs)** who are responsible for the implementation of policies that relate to the management of personal information, including policies that support compliance with privacy and data protection laws.
- **Technical Decision Makers** who determine the appropriate technology solutions to solve certain business problems.
- **IT Operations Managers** who run the systems and processes that execute the regulatory compliance program.
- **IT Security Architects** who design the IT control and security systems to provide an appropriate security level to meet the business needs of their organizations.
- **IT Infrastructure Architects** who design infrastructures that can support the IT security and controls that IT Security Architects design.
- **Consultants and partners** who implement privacy and security best practices to achieve regulatory compliance objectives for their customers.

In addition to this audience, the following individuals also might find this guide valuable:

- **Risk/Compliance Officers** who are responsible for the overall risk management of meeting compliance regulations and standards for their organizations.
- **IT Audit Managers** who are concerned with auditing IT systems and reducing the workload of internal and external IT auditors.

Caveats and Disclaimers

This guide only provides general advice about MITS compliance. Although every attempt has been made to ensure the accuracy of the information presented herein, do not rely exclusively on this guide for advice about how to address your MITS requirements.

This guidance does not constitute legal advice, and is not a substitute for individualized legal and other advice that you should receive from your legal counsel or auditors. You should always consult your team of legal advisors before you decide whether to implement the processes in this guidance to help meet the regulatory compliance obligations of your organization.

Acknowledgments

This *Microsoft MITS Compliance Planning Guide* was adapted from the work provided by the Microsoft Solutions for Security and Compliance group (MSSC) and we would like to acknowledge and thank the team that produced the *Regulatory Compliance Planning Guide*. The following people were either directly responsible or made a substantial contribution to the writing, development, and testing of the *Regulatory Compliance Planning Guide*.

Authors

Ross Carter, Microsoft
John Cobb, Wadeware LLC
Lana Earhart, Ernst & Young
Anthony Noblett, Socair Solutions
Christian Tinder, Ernst & Young

Content Contributors

Sagi Leizerov, Ernst & Young
Don McGowan, Microsoft
David Mowers, Microsoft
Richard Staynings, PricewaterhouseCoopers

Editor

Jennifer Kerns, Wadeware LLC

Program Managers

Bill Canning, Microsoft
Jeff Coon, Volt

Reviewers

Norman Barber, Microsoft
JC Cannon, Microsoft
Matt Clapham, Microsoft
Mike Danseglio, Microsoft
Scott Eagan, PricewaterhouseCoopers
Christopher Fox, PricewaterhouseCoopers
Joe Gimigliano, Purdue Pharma
Ron Hale, IT Governance Institute
Patrick Hanrion, Microsoft
Guy-Marie Joseph, Connectalk
Jason Lee, Microsoft
Brendon Lynch, Microsoft
Miles Romello, Wachovia
Brian Selby, IT Governance Institute
Ben Smith, Microsoft
Kristin Valente-Madden, Ernst & Young
Jeff Williams, Microsoft
John Wylder, Microsoft

In addition, the following individuals contributed to the development of this MITS compliance guide and their input is also greatly appreciated:

Authors

Steve Lloyd, Microsoft Canada Co.
John Weigelt, Microsoft Canada Co. Co.

Reviewers

Nadine Letson, Microsoft Canada Co.
Tina Romeo-Salem, Microsoft Canada

Content Contributors

Christian Beauclair, Microsoft Canada Co.
David Boudreau, Microsoft Canada Co.
Jamie Hart, Microsoft Canada Co.
Mike MacGillivray, Microsoft Canada Co.

Questions and/or comments regarding this guide should be directed to cangovse@microsoft.com.

Technology Solutions for Regulatory Compliance

Microsoft recognizes that departments in the Government of Canada must comply with a variety of legislation, guidelines, and policies, not just MITS. In addition, we recognize that non-government entities must contend with similar compliance issues. This section presents the technology solution categories that are relevant to regulatory compliance from a generic perspective, and identifies specific Microsoft resources that are relevant to each category (although this should not be considered to be an exhaustive list). This is followed by a mapping of major section headings in the MITS standard against the technical categories.

The Microsoft Regulatory Compliance team created and validated its list of technology solutions and their categories for them that are relevant to regulatory compliance against ISO 17799[1], the recommendations of the National Institute of Standards and Technology (NIST SP800), and other frameworks. Based on this process, the team arrived at the following 19 technology solution categories:

- Document Management
- Business Process Management
- Project Management
- Risk Assessment
- Change Management
- Network Security
- Host Control
- Malicious Software Prevention
- Application Security
- Messaging and Collaboration
- Data Classification and Protection
- Identity Management
- Authentication, Authorization, and Access Control
- Training
- Physical Security
- Vulnerability Identification
- Monitoring and Reporting
- Disaster Recovery and Failover

---

[1] ISO 17799 is a comprehensive information security management standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). These organizations derived this new standard from BS 7799 in the United Kingdom to provide an information security management framework. ISO 17799 takes a very broad approach to information security for electronic files, paper documents, recordings, and all types of communications. Although ISO 17799 is a standard and not a regulation, some regulations recommend it as the appropriate way to manage security within an organization.

- Incident Management and Trouble-Tracking

Although not included in the original 19 technical solution categories, note that a 20th technology solution category has been added to address Mobile Computing.

Each technology category is described further below, including links to additional information associated with that technology category.

Document Management

Document management solutions combine software and processes to help you manage unstructured information in your organization. This information might exist in many digital forms, including documents, engineering drawings, XML files, images, and audio and video files.

Compliance Impact

Document management targets two regulatory compliance objectives:

- Ensure that document-based policies, standards, procedures, and requirements are clearly communicated.
- Control unstructured data.

Both of these problems are issues in most compliance audits and remediation plans. Document management solutions can range from very simple to extremely complex. However, because every control category requires some form of documentation, each one requires a document management solution.

Microsoft Resources

Microsoft offers the following resources to help meet these objectives:

- **Microsoft® SharePoint® Portal Server**. This is a simple, but highly customizable document management system that integrates with Microsoft® Office to provide document and unstructured data control. For more information, see the Microsoft SharePoint Products and Technologies Web site at http://go.microsoft.com/fwlink/?linkid=12632.
- **Microsoft® Office InfoPath®**. This is an information-gathering and management program that you can use to manage unstructured Microsoft Office form data in a structured database. For more information, see InfoPath 2003 Usage Senarios at www.microsoft.com/office/infopath/prodinfo/usage/default.mspx.
- **Microsoft® Windows® Rights Management Services**. These services apply encryption-based, policy-driven protection to help organizations protect sensitive information wherever it goes. For more information, see Windows Rights Management Services at www.microsoft.com/rms.
- **Microsoft® Office**. This software is an integral part of all Microsoft-based document management solutions. It integrates documents, spreadsheets, presentations, and graphics. Office also now includes XML integration between all components in the system, which makes it easier to develop forms and direct data input from them into a database.

  For more information about:

  - How to use Microsoft® Office to streamline regulated document management, see Streamlining Regulated Document Management Using the Microsoft® Office System at www.microsoft.com/office/showcase/regulateddocument/default.mspx.
  - How to use Microsoft® Office to address the challenges of Sarbanes-Oxley, see Addressing Sarbanes-Oxley Challenges Using the Microsoft® Office System at www.microsoft.com/office/showcase/sarbanes/default.mspx.
  - How to use Microsoft® Office for contract life cycle management, see Contract Lifecycle Management for Enterprises Using the Microsoft® Office System at www.microsoft.com/office/showcase/contractlifecycle/default.mspx.
  - How to use Microsoft® Office to manage and retain documents, see Document Management and Retention for Professional Services Using the Microsoft® Office System at www.microsoft.com/office/showcase/psdocretention/default.mspx.

- How to manage healthcare documents, see Automating Clinical Forms Using the Microsoft® Office System at www.microsoft.com/office/showcase/cfa/default.mspx.
- How to remove the metadata that Microsoft Office documents collect, see The Remove Hidden Data tool for Office 2003 and Office XP Web page at http://support.microsoft.com/default.aspx?scid=kb;en-us;834427.

  Note Microsoft Office documents collect metadata about documents that you create. The metadata can contain personal information about the authors and editors of the documents, which might create compliance violations. Microsoft has created the Remove Hidden Data tool to eliminate this metadata from your documents.

Microsoft has also collaborated with independent software vendor (ISV) partners to develop document management solutions. For information about ISV partners, contact your local Microsoft sales office.

Business Process Management

Business process management (BPM) applications help provide end-to-end visibility and control over all segments of complex, multistep information requests or transactions that involve multiple applications and people in one or more organizations.

Compliance Impact

In terms of regulatory compliance, BPM helps ensure transaction security, reliable service and availability, and service level refinement. On a broader scale, BPM helps provide a messaging solution so that all affected parties involved in addressing a compliance issue are in contact and can track the issue, regardless of their physical location. Large enterprises that are subject to the Sarbanes-Oxley Act benefit most commonly from these systems.

Microsoft Resources

Business process management solutions can be simple or complex. The primary Microsoft BPM solution is Microsoft® BizTalk® Server. The following resources provide specific examples of how you can use BizTalk Server in your organization:

- For information about how to manage regulatory compliance, see Managing Regulatory Compliance with Microsoft Technology at www.microsoft.com/business/compliance.aspx.
- For more information about how BizTalk® Server can assist in providing a compliance solution, see BizTalk® Accelerator for HIPAA Web site at http://go.microsoft.com/fwlink/?linkid=12685.
- For the latest information about BizTalk® Server, see the BizTalk® Server Web site at www.microsoft.com/biztalk.

Microsoft also offers a customer relationship management (CRM) solution to help manage critical processes specific to customer interactions. For information about this solution, see the Microsoft Dynamics™ CRM Web page at www.microsoft.com/BusinessSolutions/CRM/default.mspx.

In addition, Microsoft offers Microsoft® Office Business Scorecard Manager 2005, which is a comprehensive scorecard and dashboard application that provides contextual insight into business drivers. For more information about this solution, see the Microsoft® Office® Business Scorecard Manager 2005 Web page at www.office.microsoft.com/en-us/FX012225041033.aspx.

Project Management

Project management solutions apply knowledge, skills, tools, and techniques to a broad range of activities to help meet the requirements of the particular project. Project management knowledge and practices are best described in terms of component processes. These processes divide into five process groups: envision, plan, develop, stabilize, and deploy.

Compliance Impact

Organizations use project management solutions to help implement projects, ensure operation reliability, and maintain compliance programs. Project management solutions provide additional control and feedback to project managers and other participants. These solutions provide direct cost savings, and improve project control and the effectiveness of all compliance program aspects.

Microsoft Resources

Microsoft provides the following resources for project management: the Microsoft Solutions Framework (MSF) and Microsoft® Office Project, including Project Server. Microsoft also offers the Microsoft Operations Framework (MOF), which provides guidance specifically oriented to the operation of IT organizations.

- MSF is a series of principles, models, and best practices to help project teams directly address the most common causes of project failure. MSF does not prescribe a rigid uniform project methodology, but rather allows each project team to evolve sound practices, to learn from other teams, and to take advantage of the experience of others in the IT industry. For more information, see the Microsoft Solutions Framework Web site at http://go.microsoft.com/fwlink/?linkid=45051.
- You can rapidly integrate Microsoft® Office Project 2003 in enterprises to manage and control IT projects. For more information, see the Microsoft® Office Project 2003 Web site at http://go.microsoft.com/fwlink/?linkid=29962.
- Project Server is part of the Microsoft® Office Enterprise Project Management (EPM) Solution, which includes Microsoft® Office Project Server 2003, Microsoft® Office Project Professional 2003, and Microsoft® Office Project Web Access.

  Project Server is a companion program to Project Professional. It enables online collaboration between project managers, team members, and stakeholders. Project Server also allows your organization to share standards across projects, help secure projects with check-in and check-out capability, view resource availability and resource information across projects, and manage and report on portfolios of projects.

  For more information about Project Server, see Taking advantage of Project Server Web site at http://office.microsoft.com/en-us/assistance/HA010254871033.aspx.
- For more information about MOF, see the Microsoft Operations Framework Web site at www.microsoft.com/technet/itsolutions/cits/mo/mof/default.mspx.
- For more information about enterprise project management solutions, see the Enterprise Project Management (EPM) Solution Overview at www.microsoft.com/office/project/prodinfo/epm/overview.mspx.

Risk Assessment

The term *risk assessment* can have several meanings. The information security community defines it as a systematic method to identify the assets of an information-processing system, the threats to those assets, and the vulnerability of the system to those threats. In the context of regulatory compliance, risk assessment is the process of assessing the level of compliance and compliance inadequacies within an organization.

Compliance Impact

Due to shifting requirements, most risk assessment solutions take the form of a consulting engagement that uses tools to complete the assessments. There are also methodologies your organization can use for self assessment. A critical portion of the assessment process is to identify assets and then place a qualitative or quantitative value on each asset to the enterprise.

Microsoft Resources

Microsoft offers a variety of resources for risk assessment, including solutions that analyze systems and suggest the most effective setup from a security standpoint. Microsoft also provides guidance that includes a methodology to assess risk and manage risk to IT systems.

- The *Microsoft Security Risk Management Guide* addresses how to identify assets and place a qualitative or quantitative value on each asset for the enterprise. For more information, see *The Security Risk Management Guide* at http://go.microsoft.com/fwlink/?linkid=30794.
- Microsoft® Systems Management Server (SMS) provides many methods to control network security, including such capabilities as update and hotfix management, version management, network device discovery, and monitoring. For more information about SMS, see Microsoft® Systems Management Server at www.microsoft.com/smserver/default.mspx.
- For more information about how to use additional security methods to increase the security of your Microsoft® Operations Manager (MOM) environment, see the *Microsoft Operations Manager 2005 Security Guide* at http://go.microsoft.com/fwlink/?linkid=33035.

The Microsoft Management Server group works with partners to develop IT security and regulatory compliance solutions. Some of these partners have developed specific add-on service packs that audit key compliance controls for IT resources to support compliance governance efforts. These solutions provide event collection, alert templates, and reporting services to help track auditing requirements for regulations, such as SOX, GLBA, and HIPAA.

- For more information about partner solutions for MOM, see the Management Pack and Product Connector Catalog at www.microsoft.com/management/mma/catalog.aspx.

Microsoft has also developed both a guide to help customers prevent vulnerabilities and a tool, the Microsoft® Baseline Security Analyzer (MBSA), which looks for common vulnerabilities and then notifies systems administrators to remediate them.

- For more information about security monitoring and attack detection, see *The Security Monitoring and Attack Detection Planning Guide* at www.microsoft.com/technet/security/topics/auditingandmonitoring/securitymonitoring/default.mspx.
- For more information about the MBSA tool, see the Microsoft Baseline Security Analyzer Web site at http://go.microsoft.com/fwlink/?linkid=10730.

Change Management

A *change management system* is a structured process that causes IT managers to review proposed changes for technical and business readiness in a consistent manner. The IT managers can then relax or strengthen the changes to adjust to business needs and experiences.

For example, the system for an organization could involve a database to help personnel make better decisions about future changes based on historical data that indicates the success or failure of similar changes it has tried in the past. Change management is also a structured process that communicates the status and existence of changes to all affected parties. The process can yield an inventory system that indicates what actions were taken and when that affects the status of key resources to help determine problems and resource management.

Compliance Impact

Change management is critical to regulatory compliance because it is difficult to say that your IT environment is under control if you do not know what changes have been made to it. One of the most effective ways to manage change is to use a change management solution. Such a solution, which combines software, people and processes, depends on the people and processes that it uses.

Microsoft Resources

Microsoft offers several resources for change management.

- Microsoft provides guidance for IT professionals on the basics of change management, which you also can apply to compliance. This guidance appears in the Service Management Functions (SMFs) series. For more information about change management, see the Service Management Functions: Change Management page at www.microsoft.com/technet/itsolutions/cits/mo/smf/smfchgmg.mspx.
- Microsoft® SharePoint® Services works with partner solutions to provide an example of how to control change in IT systems. For more information, see the Windows® SharePoint® Services Applications Template: Change Management download at www.microsoft.com/downloads/details.aspx?FamilyId=8481322A-88EA-44CF-9DB2-63B43A03FEB2&displaylang=en.
- The Microsoft® Office Solution Accelerator for Sarbanes-Oxley demonstrates the capability of Microsoft Office to manage the process of attaining compliance with the regulations in this act. For more information about this solution, see the Office Solution Accelerator for Sarbanes-Oxley site at http://msdn.microsoft.com/office/understanding/SOX/default.aspx.
- For information about Microsoft® Systems Management Server, which manages change on clients and servers, see Systems Management Server (SMS) at www.microsoft.com/technet/security/prodtech/SMS.mspx.

- For information about how to maintain a consistent configuration across all server roles and hardware types and ensure that all servers have required software updates, services packs, and drivers installed, see Microsoft® Systems Management Server 2003 Desired Configuration Monitoring at www.microsoft.com/technet/itsolutions/cits/mo/sman/dcm.mspx.
- Microsoft has also worked with partners to create change management solutions using Microsoft® Office. For more information about such partner solutions, contact your local Microsoft sales office.

Network Security

Network security solutions constitute a broad solution category designed to address the security of all aspects of the network for the organization, including firewalls, servers, clients, routers, switches, and access points.

Compliance Impact

Many regulations require organizations to take steps to provide appropriate security for the IT environment. Because network security is a critical element to overall information security, it is important for regulatory compliance.

Microsoft Resources

Microsoft has published a guide that provides an overview of security-related issues for networks, and describes how to plan a security monitoring system on Microsoft® Windows®–based networks. For more information, see *The Security Monitoring and Attack Detection Planning Guide* at http://go.microsoft.com/fwlink/?linkid=41309.

Microsoft has also developed guidance on general network security, network design, and protecting the perimeter of the network.

General Network Security

Microsoft has developed the following general guidance on network security:

- For information about how to secure your network, see Securing Your Network at www.microsoft.com/technet/security/topics/networksecurity/secmod88.mspx.
- For information about best practices for security, see Security Content Overview at www.microsoft.com/technet/security/bestprac/overview.mspx.
- For information about how to secure the network perimeter in small and medium businesses, see Securing Your Network: Identifying SMB Network Perimeters at www.microsoft.com/technet/security/smallbusiness/topics/networksecurity/sec_net_smb_per_dev.mspx.
- For information about how to protect against network attacks, see Protecting Clients from Network Attacks at www.microsoft.com/technet/security/smallbusiness/topics/networksecurity/prot_clients_net_attacks.mspx.
- For information about how to protect access to network assets, see Network Access Protection at www.microsoft.com/windowsserver2003/technologies/networking/nap/default.mspx.
- For information about virtual private networks, see Virtual Private Networks for Windows® Server® 2003 at www.microsoft.com/windowsserver2003/technologies/networking/vpn/default.mspx.
- For information about the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy, see Internet Authentication Service at www.microsoft.com/windowsserver2003/technologies/ias/default.mspx.

Microsoft® Systems Management Server (SMS) provides many methods to control network security, including such capabilities as update and hotfix management, version management, network device discovery, and monitoring.

- For more information about SMS, see the Microsoft® Systems Management Server site at www.microsoft.com/smserver/default.mspx.

Network Design

Microsoft has developed the following guidance on network design:

- Internet Protocol Security (IPsec) is a framework of open standards to ensure private, secure communications over IP networks that uses cryptographic security services. For more information, see IPsec at www.microsoft.com/windowsserver2003/technologies/networking/ipsec/default.mspx.
- For information about how to use IPsec and Active Directory® directory service Group Policy to isolate servers and domains, see Server and Domain Isolation Using IPsec and Group Policy at http://go.microsoft.com/fwlink/?linkid=33945.
- For information about how to use quarantine services with virtual private networks, see the *Implementing Quarantine Services with Microsoft Virtual Private Network Planning Guide* at www.microsoft.com/technet/security/prodtech/windowsserver2003/quarantineservices/default.mspx
- For information about which server products and their subcomponents in the Microsoft® Windows Server System™ use network ports and protocols, see Network Ports Used By Key Microsoft Server Products at http://go.microsoft.com/fwlink/?linkid=34291.
- For information about how to secure your network and network components, see Router and Switch Design at www.microsoft.com/technet/security/topics/networksecurity/secmod40.mspx.
- For information about how to secure remote access to network resources, see Securing Remote Access at www.microsoft.com/technet/security/smallbusiness/topics/networksecurity/sec_remote_access.mspx.
- For information about the extensive support included in Microsoft® Windows Server® 2003 and Windows® XP for the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards for high-speed networking across wireless LANs, see Wireless Networking at www.microsoft.com/technet/itsolutions/network/wifi/default.mspx.

Network Perimeter

Microsoft has developed the following guidance on protecting the network perimeter:

- For information about how to design a suitable firewall for your organization's perimeter network, see the Perimeter Firewall Design topic at www.microsoft.com/technet/security/topics/networksecurity/secmod156.mspx.
- For information about how to design a suitable firewall for your organization's internal network, see Internal Firewall Design at www.microsoft.com/technet/security/topics/networksecurity/secmod155.
- For information about configuring the Windows® Firewall feature of Windows® XP with Service Pack 2 (SP2) for individual computers, see How to Configure Windows Firewall on a Single Computer at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/cfgfwall.mspx.
- For information about how to use Group Policy to configure Windows® Firewall, see How to Configure Windows Firewall in a Small Business Environment using Group Policy at

www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/fwgrppol.mspx.

- For information about how Microsoft® Internet Security and Acceleration (ISA) Server 2004 can help provide network perimeter security, see the Microsoft Internet Security and Acceleration Server Web site at www.microsoft.com/isaserver/default.mspx.
- For information about using ISA Server 2004 in a hospital environment, see Case Studies: Hospital Increases Network Protection and Remote User Access with Security Solution at www.microsoft.com/resources/casestudies/CaseStudy.asp?CaseStudyID=15478.
- For information about using ISA Server 2004 to meet HIPAA Guidelines, see Case Studies: Iowa Hospital Meets HIPAA Compliance Guidelines with Firewall Solution at www.microsoft.com/resources/casestudies/CaseStudy.asp?CaseStudyID=15402.
- For information about using ISA Server 2000 to protect health care information in a hospital setting, see Case Studies: MemorialCare uses ISA Server to Protect Sensitive Health Information from Outsiders and Insiders at www.microsoft.com/resources/casestudies/CaseStudy.asp?CaseStudyID=13433.

Host Control

Host control solutions control the operating systems in servers and workstations. Host control solutions also include implementing security best practices at all levels of the operating system in each host, maintaining the most current updates and hotfixes, and using secure methods for daily operations.

Compliance Impact

Host control is fundamental to all of the core security control categories, such as confidentiality, integrity, and availability.

Microsoft Resources

Microsoft offers a range of resources for host control, including:

- The Microsoft® Baseline Security Analyzer (MBSA) tool that performs a best practices vulnerability assessment of the Microsoft platform. This vulnerability assessment compares existing system setup parameters against a best practice security standard. The tool notifies the IT professional of any deficiencies in the setup, which an administrator can then configure on the system.
- Another host control solution uses two Microsoft programs: Windows Server Update Services (WSUS) and Microsoft® Systems Management Server (SMS). You can use these programs separately or together, based on the size of the enterprise, and the level of automation for operating systems control.
    - WSUS, the new name for the next version of Software Update Services (SUS), is a service that automates the delivery of updates and patches to hosts running Microsoft operating systems. It has several levels of control, notifies you when updates are available, and can automatically download and install updates when they are available.
    - SMS addresses the requirements of many medium to large enterprises that need to deploy and maintain hosts with relevant software and updates, ensure hotfix management, version management, network device discovery, and monitoring.

The following sections include information about guidance Microsoft has published on basic host security, detailed host security, Microsoft® Windows Server® 2003 security, Windows® XP security, and Windows® 2000 security.

Basic Host Security

Microsoft has developed the following guidance on basic host security:

- For information about threats and countermeasures for Windows® XP and Windows Server® 2003, see the *Threats and Countermeasures Guide* at http://go.microsoft.com/fwlink/?linkid=15159.
- For information about how to secure remote client and portable computers, see Securing Remote Clients and Portable Computers at www.microsoft.com/technet/security/smallbusiness/topics/networksecurity/sec_remote_port_comp.mspx.
- For information about the MBSA tool, see the Microsoft® Baseline Security Analyzer Web site at http://go.microsoft.com/fwlink/?linkid=10730.

- For information about planning the security of services and service accounts, see *The Services and Service Accounts Security Planning Guide* at www.microsoft.com/technet/security/topics/serversecurity/serviceaccount/default.mspx.

Detailed Host Security

Microsoft has developed the following guidance on host security:

- For information about how to secure Active Directory® directory service administrative groups and accounts, see Securing Active Directory Administrative Groups and Accounts at www.microsoft.com/technet/security/smallbusiness/prodtech/activedirectory/sec_ad_admin_groups.mspx.
- For information about how to secure Internet Information Services (IIS) versions 5.0 and 5.1, see Securing Internet Information Services 5.0 and 5.1 at www.microsoft.com/technet/security/smallbusiness/prodtech/iis/sec_iis_5_0_5_1.mspx.
- For information about how to secure IIS 6.0, see Securing Internet Information Services 6.0 at www.microsoft.com/technet/security/smallbusiness/prodtech/iis/sec_iis_6_0.mspx.
- For information about how to protect against network attacks, see Protecting Clients from Network Attacks at www.microsoft.com/technet/security/smallbusiness/topics/networksecurity/prot_clients_net_attacks.mspx.
- For information about WSUS, see Windows Server Update Services at www.microsoft.com/windowsserversystem/updateservices/default.mspx
- For information about SUS, see Software Update Services (SUS) at www.microsoft.com/technet/security/prodtech/SUS.mspx.
- For information about SMS, see Systems Management Server (SMS) at www.microsoft.com/technet/security/prodtech/SMS.mspx.
- For information about security monitoring and attack detection, see *The Security Monitoring and Attack Detection Planning Guide* at www.microsoft.com/technet/security/topics/auditingandmonitoring/securitymonitoring/default.mspx.
- For information about how to use SMS 2003 for patch management, see Patch Management Using Systems Management Server 2003 at www.microsoft.com/technet/itsolutions/cits/mo/swdist/pmsms/2003/pmsms031.mspx.
- For information about how to use SUS for patch management, see Patch Management Using Microsoft Software Update Services at www.microsoft.com/technet/itsolutions/cits/mo/swdist/pmsus/pmsus251.mspx.

Windows Server® 2003 Security

Microsoft has developed the following security guidance on Windows Server® 2003:

- For information about security in Windows Server® 2003, see *Windows Server® 2003 Security Guide* at http://go.microsoft.com/fwlink/?linkid=14845.
- For information about how to secure domain controllers in a Windows Server 2003–based network, see Securing Windows Server® 2003 Domain Controllers at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsserver2003/sec_win2003_serv_dc.mspx.
- For information about how to add and secure Windows Server 2003 in a Small Business Server 2003 Active Directory domain, see Adding and Securing a Computer Running Windows Server® 2003 in a Windows® Small Business Server 2003 Active Directory Domain at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsserver2003/win2k3sbnetwork.mspx.

- For information about how to secure your Windows® Small Business Server 2003–based network, see Securing Your Small Business Server 2003 Network at www.microsoft.com/technet/security/smallbusiness/prodtech/sbs/sec_sbs2003_network.mspx.
- For information about how to use Windows® Small Business Server 2003 to add and secure a computer running Windows® XP Professional, see Adding and Securing a Computer Running Windows XP Professional by Using Windows Small Business Server 2003 at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/xp2sbs.mspx.
- For information about WSUS for Windows® Server 2003, see Windows Server Update Services at www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/wsus/default.mspx.

Windows® XP Security

Microsoft has developed the following guidance on Windows® XP security:

- For information about the features and recommended settings for Windows® XP with Service Pack 2 (SP2), see the *Windows® XP Security Guide* at http://go.microsoft.com/fwlink/?linkid=14839.
- For information about how to secure Windows® XP Professional–based client computers in a Windows Server environment, see Securing Windows XP Professional Clients in a Windows Server Environment at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/sec_winxp_pro_server_env.mspx.
- For information about configuring Windows® XP with SP2 network protection technologies in an Active Directory environment, see How to Configure Windows XP SP2 Network Protection Technologies in an Active Directory Environment at www.microsoft.com/technet/security/prodtech/windowsxp/adprtect.mspx.
- For information about configuring Windows® XP with SP2 network protection technologies in a small business environment, see How to Configure Windows XP SP2 Network Protection Technologies in a Small Business Environment at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/netprtct.mspx.
- For information about configuring Windows® XP with SP2 network protection technologies on a single computer, see How to Configure Windows XP SP2 Network Protection Technologies on a Single Computer at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/protsing.mspx.
- For information about configuring memory protection in Windows® XP with SP2, see How to Configure Memory Protection in Windows XP SP2 at www.microsoft.com/technet/security/prodtech/windowsxp/depcnfxp.mspx.

- For information about how to secure Windows® XP Professional in a peer-to-peer environment, see Securing Windows XP Professional in a Peer-to-Peer Networking Environment at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/sec_winxp_pro_p2p.mspx.
- For information about how to secure a Windows® XP Professional–based client computer in a Windows Server® 2003 domain, see Securing a Client Computer Running Microsoft Windows XP Professional in a Windows Server 2003 Active Directory Domain at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/xpwinnet.mspx.

Windows® 2000 Security

Microsoft has developed the following guidance on Windows® 2000 security:

- For information about how to secure Windows® 2000 Server, see Microsoft Solution for Securing Windows 2000 Server at http://go.microsoft.com/fwlink/?linkid=14837.
- For information about how to harden Windows® 2000, see the *Microsoft Windows 2000 Security Hardening Guide* at www.microsoft.com/technet/security/prodtech/windows2000/win2khg/01intro.mspx.
- For information about how to secure Windows® 2000 domain controllers, see Securing Windows 2000 Domain Controllers at www.microsoft.com/technet/security/smallbusiness/prodtech/windows2000/sec_win2000_serv_dc.mspx.

Malicious Software Prevention

Malicious software prevention solutions include antivirus, antispyware and antispam solutions, as well as rootkit detectors.

Compliance Impact

Without applications that you can use to help detect, monitor, and remove malicious software, there is an increased risk that sensitive corporate information in your organization could be compromised or destroyed. A lack of such resources also creates a situation in which the confidentially, integrity, and availability of the information on the IT system for your organization are increasingly at risk.

Microsoft Resources

Microsoft currently provides several tools for malicious software prevention and removal.

The Microsoft® Windows® Malicious Software Removal Tool checks computers running Windows® XP, Windows® 2000, and Windows Server® 2003 for malware infections. The tool checks for such prevalent malicious software as Zotob, RBot, Blaster, Sasser, and Mydoom, and helps remove any infections that it finds. When the detection and removal process finishes, the tool displays a report that describes the outcome, which includes information about any malicious software that was detected and removed.

Microsoft releases an updated version of this tool on the second Tuesday of each month. You can run the tool from its Web page anytime or download the tool to your computer. The tool has proven highly successful in reducing the amount of active malicious software.

- For more information, see the Malicious Software Removal Tool Web site at www.microsoft.com/malwareremove.
- For information about antispyware solutions, see the Windows Defender Web site at www.microsoft.com/athome/security/spyware/software/default.mspx.
- For information about Microsoft efforts to address spyware, see the Microsoft Security at Home: Spyware site at http://go.microsoft.com/fwlink/?linkid=47178.
- For information about how to protect servers from viruses, worms, and spam, see Help Protect Your Messaging and Collaboration Servers from Viruses, Worms, and Spam at www.microsoft.com/windowsserversystem/solutions/security/sybari.mspx.
- For information about a holistic approach to virus protection, see *The Antivirus Defense-in-Depth Guide* at www.microsoft.com/technet/security/topics/serversecurity/avdind_0.mspx.
- For security alerts and information, see Recent Security Incidents at www.microsoft.com/security/incident/default.mspx.

Application Security

Application security combines good development practices with specific software security.

Compliance Impact

Application security involves key application controls that auditors focus on as they examine critical business systems. Application security also forms a major portion of best practice recommendations, and is an area that the National Institute of Standards and Technology (NIST) Computer Security Division focuses on.

Microsoft Resources

Microsoft has developed guidance for the following aspects of application security.

Building Secure Applications

The following resources provide information on building secure applications:

- For information about how to write secure code, see Writing Secure Code, Second Edition at www.microsoft.com/mspress/books/5957.asp.
- For information about how security fits into the software development life cycle, see The Trustworthy Computing Security Development Lifecycle at www.msdn.microsoft.com/security/sdl.
- For information about how to develop secure applications, see Developing Secure Applications at www.microsoft.com/technet/security/topics/DevSecApps.mspx.
- For information about building secure ASP.NET applications, see Building Secure ASP.NET Applications: Authentication, Authorization, and Secure Communication at www.msdn.microsoft.com/library/en-us/dnnetsec/html/secnetlpMSDN.asp.
- For more information about how to improve Web application security, see Improving Web Application Security: Threats and Countermeasures at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/ThreatCounter.asp.

Application-Specific Security

Microsoft also provides guidance to improve security for specific programs, including Microsoft Exchange Server, Microsoft Systems Management Server (SMS), and Microsoft SQL Server™.

Microsoft® Exchange Server

The following resources provide information on Exchange Server:

- For information about using Windows Server® 2003 and Exchange Server 2003 to meet HIPAA security requirements, see Case Studies: Healthcare Center Improves Security and Performance with Network Upgrade at www.microsoft.com/resources/casestudies/CaseStudy.asp?CaseStudyID=16544.
- For information about planning for regulatory compliance while migrating Exchange Server, see Evaluating Factors That Affect Migration and Consolidation at www.microsoft.com/technet/itsolutions/ucs/ecm/saecm/PlanningGuide_6.mspx.
- For information about Exchange Server, see Microsoft® Exchange Server TechCenter at www.microsoft.com/technet/prodtechnol/exchange/default.mspx.
- For information about Exchange Server security and protection, see Security and Protection at www.microsoft.com/technet/prodtechnol/exchange/2003/security.mspx.
- For information about how to secure Exchange Server 2003, see Exchange Server 2003 Security Hardening Guide at http://go.microsoft.com/fwlink/?linkid=37804.

- For information about improving message security, see Exchange Server 2003 Message Security Guide at http://go.microsoft.com/fwlink/?linkid=23216.

Microsoft® Systems Management Server

The following resources provide information on Systems Management Server:

- For information about established best practices to create the most secure SMS environment possible, see Scenarios and Procedures for Microsoft Systems Management Server 2003: Security at http://go.microsoft.com/fwlink/?linkid=31433.
- For more information about SMS and its role in compliance, see the "Compliance Analysis" section of the Systems Management Server 2003 Operations Guide at www.microsoft.com/resources/documentation/sms/2003/all/opsguide/en-us/ops_3zoj.mspx.

SQL Server 2005

SQL Server 2005 includes numerous improved security features, such as:

- The permissions you can grant are far more specific than earlier versions of SQL Server.
- Nearly any object has a variety of permissions that you can grant to nearly any principal.
- You can grant or deny permissions to secure objects.

Also, in SQL Server 2005, a new set of catalog views expose all of the metadata throughout the server. From a security standpoint, a benefit of using views to expose metadata is that the data returned from a catalog view is filtered according to the permissions of the user context under which the data is requested.

The following links provide more information about SQL Server 2005:

- For IT professional information, see SQL Server 2005 on Microsoft® TechNet at www.microsoft.com/technet/prodtechnol/sql/2005/default.mspx.
- For developer information, see SQL Server 2005 on Microsoft® MSDN at http://msdn.microsoft.com/SQL/2005/default.aspx.

SQL Server 2000

The following resources provide information on SQL Server 2000:

- For information about the security features in SQL Server 2000 Service Pack 3 (SP3), see SQL Server 2000 SP3 Security Features and Best Practices at www.microsoft.com/technet/prodtechnol/sql/2000/maintain/sp3sec00.mspx.
- For information about SQL Server 2000 partners for security solutions, see Partners for Security Solutions at www.mssqlpartnerdirectory.com.

Messaging and Collaboration

Messaging and collaboration applications have become essential tools. Collaboration applications can range from integrated document programs, such as Microsoft® Office to portals, instant messaging, online presentation software, and peer-to-peer programs.

Compliance Impact

One of the most common issues that most regulatory compliance assessments find is that messaging applications, such as e-mail, expose privileged information outside the organization. Because e-mail is so ubiquitous and employees rely on it so heavily to perform their jobs, automating the protection of messaging and collaboration solutions is essential.

Messaging and collaboration programs provide a large productivity improvement for teams engaged in achieving compliance objectives, and they add to the overall efficiency of the organization. In addition, information that auditors or internal resources gather during assessments must be transferable to the teams that perform the actual fix installations or later remediation activities. Collaboration solutions such as portals improve the efficiency of the information sharing.

Microsoft Resources

Common methods to help prevent messaging security breaches include messaging gateways, secure messaging servers, and messaging content filtration. Both messaging gateways and messaging content filtration route messages to a specialized software application that uses statistical and language-based methods to isolate specific word or number strings. Messages that contain these key words or strings generally are then placed in quarantine until the suspect information in the messages can be verified. For guidance on helping to secure both messaging and collaboration servers, see Help Protect Your Messaging and Collaboration Servers from Viruses, Worms, and Spam at www.microsoft.com/windowsserversystem/solutions/security/sybari.mspx.

Messaging Services

In addition to the traditional e-mail messaging system that Microsoft provides with Microsoft® Office Outlook® and Exchange Server, Microsoft also provides enterprise instant messaging, and other services through Office Communicator and Live Communications Server.

Microsoft® Exchange Server

The following resources provide information on the security and compliance capabilities in Microsoft® Exchange Server:

- For information about Exchange Server 2003 security, see Secure Messaging with Microsoft® Exchange Server 2003 by Paul Robichaux, published by Microsoft Press 2004 at www.microsoft.com/mspress/books/6893.asp.
- For information about Exchange Server, see Microsoft Exchange Server TechCenter at www.microsoft.com/technet/prodtechnol/exchange/default.mspx.
- For information about Exchange Server security and protection, see Security and Protection at www.microsoft.com/technet/prodtechnol/exchange/2003/security.mspx.
- For information about how to secure e-mail on Microsoft Exchange Server 2003, see the *Exchange Server 2003 Message Security Guide* at http://go.microsoft.com/fwlink/?linkid=23216.

- For information about how to use Microsoft® Office Outlook 2003 to limit junk e-mail messages, see Using Microsoft Office Outlook 2003 to Limit Junk E-Mail Messages at www.microsoft.com/technet/security/smallbusiness/prodtech/office/spamout.mspx.
- For information about securing Exchange Server 2003, see *Exchange Server 2003 Security Hardening Guide* at http://go.microsoft.com/fwlink/?linkid=37804.
- For information about using Microsoft® Windows Server® 2003 and Exchange Server 2003 to meet HIPAA security requirements, see Case Studies: Healthcare Center Improves Security and Performance with Network Upgrade at www.microsoft.com/resources/casestudies/CaseStudy.asp?CaseStudyID=16544.
- For information about planning for regulatory compliance while migrating Exchange, see Evaluating Factors That Affect Migration and Consolidation at www.microsoft.com/technet/itsolutions/ucs/ecm/saecm/PlanningGuide_6.mspx.
- For information about supporting regulatory compliance with Exchange Server 2003, see Supporting Regulatory Compliance with Exchange Server 2003 at www.microsoft.com/exchange/evaluation/compliance.mspx.
- For information about the journaling feature in Exchange Server 2003, see Overview of Exchange Server 2003 Journaling at www.microsoft.com/technet/prodtechnol/exchange/guides/E2k3Journal.

Office Communicator

- For information about Microsoft® Office Communicator 2005, see Microsoft Office Communicator 2005 Help at http://office.microsoft.com/en-us/assistance/HP011725551033.aspx.

Live Communications Server 2005

- For information about Live Communications Server, see Live Communications Server Product Information at www.microsoft.com/office/livecomm/prodinfo/default.mspx.

Microsoft® Exchange Hosted Services

Microsoft Exchange Hosted Services helps address corporate e-mail security, compliance, and availability requirements.

- For more information about Microsoft Exchange Hosted Services, see Microsoft Exchange Hosted Services at www.microsoft.com/exchange/services/default.mspx.

Collaboration Services

Microsoft has developed a series of programs to help knowledge workers collaborate. These programs integrate parts of the Microsoft Office Suite such as SharePoint® Portal Server, Live Communications Server 2005, InfoPath®, OneNote®, and Project Server. In addition, Windows SharePoint Services, which is a streamlined version of SharePoint Portal Services, is included in the basic Windows Server 2003 package.

SharePoint® Services and SharePoint® Portal Server

The following resources provide information about this service and application:

- For more information about SharePoint® Services and SharePoint® Portal Server, see Microsoft SharePoint Products and Technologies at http://go.microsoft.com/fwlink/?linkid=46807.
- For information about how to design, deploy, customize, and troubleshoot SharePoint products and technologies, see the Microsoft SharePoint Products and Technologies Resource Kit at www.microsoft.com/technet/prodtechnol/sppt/reskit/default.mspx.
- For information about Windows® SharePoint® Services, see Windows SharePoint Services at www.microsoft.com/WindowsServer2003/technologies/sharepoint/default.mspx.

Live Meeting

- For information about Live Meeting, see the Live Meeting Product Information page at www.microsoft.com/office/livemeeting/prodinfo/default.mspx.

Office Communicator

- For information about Microsoft® Office Communicator 2005, see Microsoft Office Communicator 2005 Help at http://office.microsoft.com/en-us/assistance/HP011725551033.aspx.

Live Communications Server 2005

- For more information about Live Communications Server, see Live Communications Server Product Information at www.microsoft.com/office/livecomm/prodinfo/default.mspx.

InfoPath® 2003

- For more information about InfoPath® 2003, see InfoPath® 2003 Product Information at www.microsoft.com/office/infopath/prodinfo/default.mspx.

OneNote® 2003

- For more information about OneNote®, see the OneNote Product Information site at www.microsoft.com/office/onenote/prodinfo/default.mspx.

Project Server 2003

- For more information about Project Server, see the Project Server 2003 Technical Library at www.microsoft.com/technet/prodtechnol/office/proj2003/reskit/default.mspx.

Messaging and Collaboration Anti-Malware Software

- For more information about how to protect your messaging and collaboration servers from viruses, worms, and spam, see Help Protect Your Messaging and Collaboration Servers from Viruses, Worms, and Spam at www.microsoft.com/windowsserversystem/solutions/security/sybari.mspx.
- For more information about Microsoft's defense-in-depth approach to help protect enterprises against malware, see http://www.microsoft.com/securemessaging/default.mspx.

Groove

Microsoft acquired Groove Networks in early 2005. Groove Virtual Office provides software that allows a team to work together as if all members were in the same physical location. The software enables teams to perform various tasks from simple file sharing, to running formal and informal projects, to large-scale business processes. Groove 4.0 is expected to include document management improvements to more closely integrate the software with Office 12 and Windows SharePoint Services.

For more information about Groove, see Products: Why Groove at www.groove.net/index.cfm?pagename=Products_Overview.

Data Classification and Protection

Data classification and protection deals with how to apply security classification levels to the data either on a system or in transmission. This solution category also deals with data protection in terms of providing confidentiality and integrity to data that is either at rest or in transmission. Cryptographic solutions are the most common method that organizations use to provide data protection.

Compliance Impact

Data classification is important to compliance because it informs users about what levels indicate the relative importance of the data, how they must handle the data, and how they must safeguard and dispose of it. High, medium, and low are typical data classification examples that indicate the relative impact of the data on business. The military classification system of Top Secret, Secret, Confidential, and Un-Classified may also apply in some organizations.

All compliance guidelines require file protection and encryption of sensitive information, whether at rest or in transit. The compliance process creates enormous amounts of sensitive data, primarily in nonstructured applications, such as Microsoft® Word and Excel® files. Control and protection of this compliance data is very important because it contains complete details of an organization's known weaknesses and vulnerabilities.

Microsoft Resources

Microsoft provides several resources for data classification and data protection. For example, the combined use of Information Rights Management (IRM), which extends the Windows Rights Management Services in Microsoft® Office 2003 applications and in Microsoft® Internet Explorer®, as well as Windows® Rights Management Services (RMS) technologies help you to both classify and help protect the data in your organization. RMS applies encryption-based, policy-driven protection that travels with the information wherever it goes.

Additional data protection technology examples include Internet Protocol security (IPsec) and Encrypting File System (EFS). IPsec provides data integrity and encryption to IP traffic, whereas EFS encrypts files stored in the file systems of Microsoft® Windows® 2000, Windows® XP Professional, and Windows Server® 2003. Microsoft provides the following guidance on these data classification and protection solutions.

- For more information about Windows® Rights Management Services partner offerings, see Windows Rights Management Services partners at www.microsoft.com/windowsserver2003/partners/rmspartners.mspx.
- For more information about RMS, see Windows Rights Management Services at www.microsoft.com/rms.
- For more information about the information rights management capabilities of Office 2003, see Information Rights Management in Microsoft® Office 2003 at www.microsoft.com/technet/prodtechnol/office/office2003/operate/of03irm.mspx.
- For information about IPsec, see the IPsec Web site at www.microsoft.com/windowsserver2003/technologies/networking/ipsec/default.mspx.
- For information about how to use IPsec and Group Policy to isolate servers and domains, see Server and Domain Isolation Using IPsec and Group Policy at http://go.microsoft.com/fwlink/?linkid=33945.
- For information about how to use EFS to protect data, see Protecting Data by Using EFS to Encrypt Hard Drives at www.microsoft.com/technet/security/smallbusiness/topics/cryptographyetc/protect_data_efs.mspx.

- For more information about EFS, see The Encrypting File System http://go.microsoft.com/fwlink/?linkid=46681.
- For information about how to protect sensitive information from theft, see Protecting Sensitive Information from Theft on Windows® XP Professional in a Workgroup at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/efsxppro.mspx.
- For more information about full volume encryption available with Windows Vista Enterprise edition (availability scheduled for the end of 2006), see the BitLocker™ Executive Overview at http://www.microsoft.com/technet/windowsvista/security/bitexec.mspx or the BitLocker™ Technical Overview at http://www.microsoft.com/technet/windowsvista/security/bittech.mspx.

Identity Management

In an information network, the organization uses identity management software and processes to help manage users' digital identities and their digital entitlements.

Compliance Impact

This solution category applies to many of the critical control categories in regulatory compliance. Identity management solutions are one of the top recommendations from consultants to help meet regulatory compliance requirements. Examples of identity management solutions include developing processes to ensure accounts are disabled in a timely fashion, and developing processes to review the access controls on data resources.

Microsoft Resources

Identity management offerings from Microsoft include Microsoft® Windows® 2000 Server, Windows Server® 2003 with the Active Directory® directory service, Microsoft® Identity Integration Server (MIIS 2003), and Public Key Infrastructure (PKI) for Windows Server® 2003. MIIS 2003 provides overall control of an enterprise identity.

General Concepts

Microsoft provides the following general guidance on identity management solutions:

- For fundamental information about identity management, see the "Fundamental Concepts" paper of the *Identity and Access Management Series* at www.microsoft.com/technet/security/topics/identitymanagement/idmanage/P1Fund_0.mspx.
- For information about identity management platform and infrastructure, see the "Platform and Infrastructure" paper at www.microsoft.com/technet/security/topics/identitymanagement/idmanage/P1Plat_0.mspx.
- For information about intranet access management, see the "Intranet Access Management" paper at www.microsoft.com/technet/security/topics/identitymanagement/idmanage/P3Intran_0.mspx.
- For information about extranet access management, see the "Extranet Access Management" paper at www.microsoft.com/technet/security/topics/identitymanagement/idmanage/P3Extran_0.mspx.
- For information about identity aggregation and synchronization, see the "Identity Aggregation and Synchronization" paper at www.microsoft.com/technet/security/topics/identitymanagement/idmanage/P2Ident_0.mspx.
- For information about the security of services and service accounts, see *The Services and Service Accounts Security Planning Guide* at www.microsoft.com/technet/security/topics/serversecurity/serviceaccount/default.mspx.

Specific Examples

Microsoft provides the following specific examples on identity management solutions:

- For information about directory services administration, see Service Management Functions: Directory Services Administration at www.microsoft.com/technet/itsolutions/cits/mo/smf/smfdirsa.mspx.
- For information about deploying and operating a PKI, see Deploying PKI Inside Microsoft at www.microsoft.com/technet/itsolutions/msit/security/deppkiin.mspx.
- For information about how to secure Active Directory administrative groups and accounts, see Securing Active Directory Administrative Groups and Accounts at www.microsoft.com/technet/security/smallbusiness/prodtech/activedirectory/sec_ad_admin_groups.mspx.
- For information about how to build an enterprise root CA in small and medium businesses, see Building an Enterprise Root Certification Authority in Small and Medium Businesses at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsserver2003/build_ent_root_ca.mspx.
- For information about Active Directory, see http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx.
- For information about Active Directory Federation Services (ADFS), see http://www.microsoft.com/WindowsServer2003/R2/Identity_Management/ADFSwhitepaper.mspx.
- For more information about PKI for Windows 2003, see http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx.
- For information about Microsoft's Certificate Lifecycle Manager (CLM) that helps organizations manage the lifecycle of digital certificates and smart cards, see http://www.microsoft.com/windowsserversystem/CLM/overview.mspx.

Authentication, Authorization, and Access Control

Authentication usually involves a user name and a password, but it can include additional methods to demonstrate identity, such as a smart card, retina scan, voice recognition, or fingerprints. Authorization focuses on determining if someone, after the person is identified, is permitted to access requested resources. Access is granted or denied depending on a wide variety of criteria, such as the network address of the client, the time of day, or the browser that the person uses.

Compliance Impact

This control objective is critical to helping to meet the requirements of the core security principles of confidentiality, integrity, and availability.

Microsoft Resources

Much of the Active Directory® directory service within the Microsoft® Windows® 2000 Server and Windows Server® 2003 operating systems focuses on authentication, authorization, and access control. Internet Authentication Service (IAS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy.

As a RADIUS server, IAS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless and virtual private network (VPN) connections. As a RADIUS proxy, IAS forwards authentication and accounting messages to other RADIUS servers.

General Concepts

Microsoft provides the following general guidance on these control solutions:

- For information about securing administrator accounts, see *The Administrator Accounts Security Planning Guide* at www.microsoft.com/technet/security/topics/serversecurity/administratoraccounts/default.mspx
- For information about how to select secure passwords, see Selecting Secure Passwords at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/select_sec_passwords.mspx.
- For information about how to enforce strong password usage, see Enforcing Strong Password Usage Throughout Your Organization at www.microsoft.com/technet/security/smallbusiness/topics/networksecurity/enforce_strong_passwords.mspx.
- For more information on the Microsoft Identity and Access Management Strategy, see Microsoft Identity and Access Management Series at http://www.microsoft.com/technet/security/topics/identitymanagement/idmanage/default.mspx?mfr=true.
- For information on helping secure Active Directory, 19 Smart Tips for Securing Active Directory at http://www.microsoft.com/technet/technetmag/issues/2006/05/SmartTips/default.aspx .
- For information about deploying and operating public key infrastructure (PKI), see Deploying PKI Inside Microsoft at www.microsoft.com/technet/itsolutions/msit/security/deppkiin.mspx.

- For information about how to build an enterprise root certification authority in small and medium businesses, see Building an Enterprise Root Certification Authority in Small and Medium Businesses at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsserver2003/build_ent_root_ca.mspx.
- For more information about PKI for Windows 2003, see http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx.
- For process and technical guidance for consolidating security and directory services to provide authentication and authorization in heterogeneous UNIX and Windows environments using Windows Server 2003, see Solution Guide for Windows Security and Directory Services for UNIX at http://www.microsoft.com/downloads/details.aspx?FamilyId=144f7b82-65cf-4105-b60c-44515299797d&displaylang=en.

Specific Examples

Microsoft provides the following specific examples on these control solutions:

- For information about using IAS, see Internet Authentication Service at www.microsoft.com/technet/itsolutions/network/ias/default.mspx.
- For information about how to use smart cards to secure access, see *The Secure Access Using Smart Cards Planning Guide* at www.microsoft.com/technet/security/topics/networksecurity/securesmartcards/default.mspx.
- For information about using certificate services to secure wireless local area networks, see Securing Wireless LANs with Certificate Services at http://go.microsoft.com/fwlink/?linkid=14843.
- For information about using Protected Extensible Authentication Protocol (PEAP) and passwords to secure wireless LANs, see Securing Wireless LANs with PEAP and Passwords at http://go.microsoft.com/fwlink/?linkid=23459.
- For information about security features such as User Account Control with Windows Vista Enterprise (to be available in Q4 CY2006), see http://www.microsoft.com/technet/windowsvista/evaluate/feat/secfeat.mspx.

Training

It is vital to the overall success of the organization to familiarize employees by providing training on requirements and processes specific to security and compliance. Training provides the critical link between people, processes, and technologies that make a security program work.

Compliance Impact

Regulatory compliance demands that organizations address security and compliance training. Security and compliance training solutions in most organizations are typically modifications of existing training software solutions.

Microsoft Resources

Microsoft and its partners provide training solutions through the following resources that you can modify to help meet the security and compliance requirements in this area for your organization:

- For more information about Microsoft training, see Microsoft Training Overview at www.microsoft.com/learning/training/default.asp.
- For more information about Microsoft Office training, see Microsoft Office Training Home Page at http://office.microsoft.com/en-us/training/default.aspx.
- For more information about workforce management, see Service Management Functions: Workforce Management at www.microsoft.com/technet/itsolutions/cits/mo/smf/smfwrkmg.mspx.

Physical Security

Physical security solutions secure physical access and control of the systems and workstations in your organization.

Compliance Impact

Physical security is critical to help ensure the security of the entire IT environment in the organization. This is because attacks in which the attacker gains physical access to the server almost always succeed in compromising the organization's resources. Qualified service providers usually custom-develop physical security solutions for the organization, as well as install and provide support services for them.

Microsoft Resources

Although Microsoft does not provide physical security resources, it does provide guidance on how to provide secure access using smart cards.

For more information, see *The Secure Access Using Smart Cards Planning Guide* at www.microsoft.com/technet/security/topics/networksecurity/securesmartcards/default.mspx.

Vulnerability Identification

Vulnerability identification solutions provide tools that you can use to help test for vulnerabilities in your organization's information systems. IT personnel must be aware of vulnerabilities in the IT environment before they can effectively address them.

Compliance Impact

Regularly monitoring computers and servers for vulnerabilities in the organization is extremely important because it provides a controlled platform on which to run business application software. If IT management is unaware of the vulnerabilities that exist in the organization's systems, management cannot be sure whether an attacker has compromised the environment. A compromised environment is not under control, making it unsuitable to run business software that is compliant.

Microsoft Resources

The Microsoft® Baseline Security Analyzer (MBSA) performs a best practices vulnerability assessment for the Microsoft platform. This vulnerability assessment tool compares existing setup parameters on a system against a security best practice standard.

The MBSA tool notifies IT personnel of certain deficiencies in the system setup, which they can then manually configure. Microsoft Baseline Security Analyzer (MBSA) 2.0 is an easy-to-use tool that helps small and medium businesses determine their security state in accordance with Microsoft security recommendations, and this tool also offers specific remediation guidance.

You can improve your security management process by using MBSA to detect common security misconfigurations and missing security updates on your computer systems. The tool, which is built on the Microsoft® Windows® Update Agent and Microsoft Update infrastructure, helps ensure consistency with other Microsoft management products, including Microsoft Update, Windows Server Update Services, Microsoft Systems Management Server, and Microsoft Operations Manager.

- For more information about the MBSA tool, see the Microsoft Baseline Security Analyzer Web site at http://go.microsoft.com/fwlink/?linkid=10730.

Microsoft also has produced a security monitoring and attack detection guide for security professionals that provides information on the detection and monitoring process.

- For more information about this resource, see *The Security Monitoring and Attack Detection Planning Guide* at www.microsoft.com/technet/security/topics/auditingandmonitoring/securitymonitoring/default.mspx.

Monitoring and Reporting

Monitoring and reporting solutions collect and audit logs that result from authentication and access to systems. These solutions are either designed to collect specific information based on compliance to certain regulations, or use existing logs built into operating systems or software packages.

A subcategory of monitoring and reporting is the collection, analysis, and correlation of all logged data across the organization. This is sometimes accomplished through a dashboard-type solution, where you can better analyze the various information gathered throughout the organization. This type of solution allows IT management to better determine if there is a correlation between events.

Compliance Impact

Monitoring and reporting solutions provide verification and quality control methods to ensure that organizations maintain security and confidentiality. For example, these solutions can assist your organization in its efforts to comply with HIPAA, which requires auditors to evaluate individual patient records.

Microsoft Resources

All current Microsoft operating systems include logging capabilities. For more information about these capabilities, see the operating system documentation. Microsoft® Operations Manager (MOM) is designed to enhance this built-in capability.

- For more information about MOM security, see the *Microsoft Operations Manager 2005 Security Guide* at http://go.microsoft.com/fwlink/?linkid=33035.
- In addition, the next version of MOM (named System Center Operations Manager 2007) will include a security event audit feature for capturing and reporting on security events. To obtain additional information, see http://www.microsoft.com/mom/evaluation/beta/opsmgroverview.mspx.

Systems Management Server (SMS) 2003 Desired Configuration Monitoring is a powerful solution to monitor configuration settings across most server roles and hardware types for non-compliance. Administrators can define desired configuration models with templates and enable SMS 2003 to proactively view non-compliance in the WMI, Active Directory, IIS Metabase, Registry, and File System settings. The SMS 2003 solution will alert the administrator when non-compliance is detected from the predefined desired configuration.

- For more information about SMS 2003 DCM, see the *Microsoft Systems Management Server 2003 Desired Configuration Monitoring* at http://www.microsoft.com/downloads/details.aspx?familyid=93A72AB8-BF54-4607-B9BB-AC9739C6C292&displaylang=en.

The Microsoft® Management Server group has worked with partners to develop IT security and regulatory compliance solutions. Two of these partners have developed specific add-on packs that audit key compliance controls for IT resources to support compliance governance efforts. The add-on packs provide event collection, alert templates, and reporting services to track monitoring and reporting requirements for regulations, such as SOX, GLBA, and HIPAA.

- For more information on MOM partners and the add-on packs, see the Management Pack and Product Connector Catalog at www.microsoft.com/management/mma/catalog.aspx.

Microsoft® Windows® Rights Management Services (RMS) applies encryption-based, policy-driven protection that travels with information wherever it goes to help organizations protect sensitive information. RMS creates a log entry for every server

action, including such events as new users obtaining RMS credentials, and newly protected content consumption. This information can be very helpful to organizations developing monitoring and reporting solutions.

- For more information about RMS, see the Windows Rights Management Services site at www.microsoft.com/rms.
- For more information about the Microsoft Office Excel® add-in for SQL Server Analysis Services, see Office Excel Add-in for SQL Server Analyis Services at www.microsoft.com/office/solutions/accelerators/exceladdin/default.mspx.
- For more information about Microsoft SQL Server™ 2000 Reporting Services, see the SQL Server 2000 Reporting Services site at www.microsoft.com/sql/reporting/default.mspx.
- For information about the security features of SQL Server 2000 SP3, see SQL Server 2000 SP3 Security Features and Best Practices at www.microsoft.com/technet/prodtechnol/sql/2000/maintain/sp3sec00.mspx.

For additional dashboard type reporting solutions, see the following resources:

- For information about dashboard and reporting services from Microsoft partners, see Component Partners for Reporting Services at www.microsoft.com/sql/reporting/partners/component.asp.
- For more information about building financial reporting dashboards see Building Financial Reporting Dashboards Using the Microsoft® Office System at www.microsoft.com/office/showcase/findashboard/default.mspx.
- For information about business intelligence for reporting services from Microsoft partners, see Business Intelligence Partners for Reporting Services at www.microsoft.com/sql/reporting/partners/bi.asp.

Disaster Recovery and Failover

In the event of a natural or man-made disaster, the information systems for the organization must return to an operational state as quickly as possible. *Disaster recovery and failover* are terms that relate to this process. Failover refers to redundant systems that operate in parallel to the operational systems at all times. It is preferable to disperse these systems geographically.

One way to provide redundancy is to implement systems that are inherently protected from certain kinds of failure. Such systems include the multimaster Active Directory® directory service, clustered SQL Server, and Microsoft® Windows Server® Network Load Balancing and Cluster Service (MSCS) technology.

Compliance Impact

Many regulations and standards explicitly require disaster recovery and failover solutions, including HIPAA, GLBA, and EUDPD.

Microsoft Resources

Microsoft provides specific guidance on disaster recovery (also known as business continuity) and failover solutions.

Backup and Recovery

The following resources provide information on backup and recovery:

- Data Protection Manager (DPM) is the new Microsoft server software solution for rapid and reliable data recovery. For information about DPM, see Microsoft System Center Data Protection Manager at www.microsoft.com/windowsserversystem/dpm/default.mspx.
- For information about Exchange Server disaster recovery, see the Exchange Server Disaster Recovery Analyzer Web page at www.microsoft.com/downloads/details.aspx?familyid=C86FA454-416C-4751-BD0E-5D945B8C107B&displaylang=en.
- For information about disaster recovery, see Disaster Recovery at www.microsoft.com/technet/security/topics/disasterrecovery.
- For information about how to back up and recover data, see Backing Up and Recovering Data at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsserver2003/backup_restore_data.mspx.
- For information about how to back up and restore data from Windows Server 2003, see Backing Up and Restoring Data for Windows Server® 2003 at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsserver2003/ntbackup.mspx.
- For information about how to back up and restore Windows Small Business Server 2003, see Backing Up and Restoring Windows Small Business Server 2003 at www.microsoft.com/technet/security/smallbusiness/prodtech/sbs/backup_restore_sbs2003.mspx.
- For information about how to back up and restore data for Windows 2000 Server, see Backing Up and Restoring Data for Windows® 2000 Server at www.microsoft.com/technet/security/smallbusiness/prodtech/windows2000/backupwin2k.mspx.
- For information about storage management, see Service Management Functions: Storage Management at www.microsoft.com/technet/itsolutions/cits/mo/smf/smfstomg.mspx.

- For information about service continuity management, see Service Management Functions: Service Continuity Management at www.microsoft.com/technet/itsolutions/cits/mo/smf/smfsrcmg.mspx.
- For a disaster recovery preparation worksheet for Exchange Server 2003, see http://www.microsoft.com/technet/prodtechnol/exchange/2003/drchecklist.mspx.
- For information about SharePoint Disaster Prevention and Recovery, see http://www.microsoft.com/technet/technetmag/issues/2005/11/BePrepared/default.aspx and http://www.microsoft.com/technet/prodtechnol/sppt/reskit/c2861881x.mspx.

Redundant Systems

The following resources provide information about Microsoft components and solutions for redundancy:

- For information about multimaster Active Directory, see the What is the Active Directory Replication Model topic at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ad/ad/what_is_the_active_directory_replication_model.asp.
- For information about clustered SQL Server, see SQL Server 2000 Failover Clustering at www.microsoft.com/technet/prodtechnol/sql/2000/maintain/failclus.mspx.
- For information about Network Load Balancing, see Windows Server® 2003 Network Load Balancing (NLB) at www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/nlb.mspx.
- For information about Windows Server 2003 cluster technology, see Clustering Services at www.microsoft.com/windowsserver2003/technologies/clustering/default.mspx.

Incident Management and Trouble-Tracking

Incident management and trouble-tracking solutions use customized systems that manage specific business processes from beginning to end. The actual system functionality closely matches the Customer Relationship Management (CRM) business application category.

Compliance Impact

Several regulations and standards, including GLBA and HIPAA, specifically require organizations to use incident management and trouble-tracking solutions.

Microsoft Resources

The following guidance from Microsoft is available on incident management and trouble-tracking:

- For information about how to respond to IT security incidents, see Responding to IT Security Incidents at www.microsoft.com/technet/security/topics/disasterrecovery/responding_sec_incidents.mspx.
- For information about problem management, see Service Management Functions: Problem Management at www.microsoft.com/technet/itsolutions/cits/mo/smf/smfprbmg.mspx.
- For information about incident management, see Service Management Functions: Incident Mangement at www.microsoft.com/technet/itsolutions/cits/mo/smf/smfincmg.mspx.
- For information about service desk functions, see Service Management Functions: Service Desk at www.microsoft.com/technet/itsolutions/cits/mo/smf/smfsvcdk.mspx.
- For more information about how to respond to incidents, see *Windows Security Resource Kit* Second Edition 2005, by Smith and Komar, from Microsoft Press at www.microsoft.com/mspress/books/6418.asp.
- Microsoft provides a solution accelerator for auto-ticketing for organizations that have deployed (or are considering deploying) MOM 2005. For more information, see Autoticketing Solution Accelerator at http://www.microsoft.com/technet/itsolutions/cits/mo/smc/as05.mspx.
- For information on automatically creating tickets in 3rd party Service Desk products based on alerts received within MOM, see Microsoft Operations Manager Product Connectors at http://www.microsoft.com/management/momprodconnectors.mspx.

Mobile Computing

Overview

The Enterprise workforce is becoming increasingly mobile, accessing corporate information whenever and where required. It is essential that the mobile information worker and their solutions are included within the compliance program.

Compliance Impact

Mobile information assets must be addressed to ensure a comprehensive regulatory compliance program. Mobile compliance solutions are typically extensions of existing compliance solutions, but take the periodic connectivity of mobile devices into consideration.

Microsoft Solution

Microsoft and its partners provide solutions to assist withr security and compliance:

- For information about how to protect access to network assets, see Network Access Protection at www.microsoft.com/windowsserver2003/technologies/networking/nap/default.mspx.
- For more information about Windows mobile devices and security, see http://www.microsoft.com/windowsmobile/business/strategy/security.mspx.
- For more information about Windows Mobile 5.0 Application Security, see http://msdn.microsoft.com/mobility/default.aspx?pull=/library/en-us/dnppcgen/html/wmsecurity.asp.
- For more information on Microsoft Exchange 2003 SP2 Messaging and Security Featurepack, see http://www.microsoft.com/windowsmobile/business/5/default.mspx
- For information on Microsoft Systems Management Server, Device Management Feature Pack, see http://www.microsoft.com/smserver/downloads/2003/dmfp.asp.

Summary

This section provides a description of technology solutions that organizations use to help achieve and maintain compliance. It discusses the reasons these solutions are important, and offers links to Microsoft guidance and technology that can help your organization toward achieving regulatory compliance mandates.

The effect of implementing these solutions not only helps to provide security and compliance standards for your IT environment, but also has a positive affect on the organization's business processes. Before you implement any of the identified solutions, be sure to meet with your legal advisors and auditors to obtain legal advice about your own unique compliance needs, and carefully consider the impact of these solutions on the entire organization, not just in terms of compliance. Microsoft is committed to providing more in-depth research and solutions for regulatory compliance. However, you can also search publicly to pursue more information on this complex and important subject.

Mapping of MITS Sections against Technical Solution Categories

Table 1 provides a mapping of relevant section headings in the MITS standard against the technical solution categories discussed above. Note that not all section headings are identified in this table as non-applicable sections have been omitted. Also note that a referenced technology solution category section does not necessarily apply in its entirety. The detailed MITS compliance matrix provided in Appendix A can be consulted for specific items that apply to specific mandatory requirements.

Table 1: Mapping MITS and Technology Solution Categories

	Document Management	Business Process Management	Project Management	Risk Assessment	Change Management	Network Security	Host Control	Malicious Software Prevention	Application Security	Messaging and Collaboration	Data Classification and Protection	Identity Management	Authentication, Authorization & Access Control	Physical Security	Training	Vulnerability Identification	Monitoring and Reporting	Disaster Recovery and Failover	Incident Management and Trouble-Tracking	Mobile Computing
9.1 IT Security Coordinator	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü
9.2 Senior Management	ü	ü	ü																	
9.3 Departmental Security Officer	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü
9.4 Chief Information Officer	ü	ü	ü																	
9.5 Business Continuity Planning Coordinator	ü	ü	ü															ü		
9.6 Program and Service Delivery Managers	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü
9.7 IT Operational Personnel	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü
9.8 Other Personnel	ü	ü	ü											ü						
9.9 COMSEC Custodian	ü	ü	ü								ü									
9.10 IT Project Managers	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü
10. Departmental IT Security Policy	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü
11. IT Security Resources for Projects	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü
12.1 Security in the System Development Life Cycle				ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü
12.2 Identification and Categorization of Information and IT Assets				ü																
12.3 Security Risk Management	ü	ü	ü	ü	ü												ü			
12.3.2 Threat and Risk Assessment	ü	ü	ü	ü	ü	ü											ü			
12.3.3 Certification and Accreditation	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü
12.5 Vulnerability Management				ü			ü									ü	ü		ü	
12.5.1 Vulnerability Assessments				ü			ü													
12.5.2 Patch Management							ü													
12.6 Segregation of Responsibilities													ü	ü						
12.8 Continuity Planning	ü	ü	ü															ü		
12.10 Sharing and Exchange of Information and IT Assets										ü	ü		ü	ü						
12.11 Departmental IT Security Assessment and Audit	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü
12.11.1 Self-Assessment	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü
12.11.2 Internal Audit	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü

Table 1 : Mapping MITS and Technology Solution Categories

	Document Management	Business Process Management	Project Management	Risk Assessment	Change Management	Network Security	Host Control	Malicious Software Prevention	Application Security	Messaging and Collaboration	Data Classification and Protection	Identity Management	Authentication, Authorization & Access Control	Physical Security	Training	Vulnerability Identification	Monitoring and Reporting	Disaster Recovery and Failover	Incident Management and Trouble-Tracking	Mobile Computing
12.12 IT Security Awareness															ü					
12.13 IT Security Training															ü					
13. Graduated Safeguards				ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	
14.1 Configuration Management and Change Control					ü															
14.2 Problem Reporting/Help Desk																		ü		
14.3 System Support Services																	ü			
15. Active Defence Strategy	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	
16.1 Physical Security within the IT Security Environment											ü		ü							
16.2 Storage, Disposal and Destruction of IT Media											ü									
16.3 Personnel Security within the IT Security Environment																				
16.4.1 Selection of Security Products	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	ü	
16.4.2 Identification and Authentication												ü								
16.4.3 Authorization and Access Control													ü							
16.4.4 Cryptography											ü									
16.4.5 Public Key Infrastructure												ü	ü							
16.4.6 Network Security and Perimeter Defence						ü											ü			
16.4.7 Mobile Computing and Teleworking						ü							ü							
16.4.8 Wireless Devices															ü					ü
16.4.11 Software Integrity and Security Configuration							ü													
16.4.12 Malicious Code								ü												
17. Detection																ü	ü		ü	
18. Response and Recovery																		ü	ü	
18.3 Incident Response																		ü		
18.4 Incident Reporting																			ü	
18.5 Recovery					ü													ü		
18.6 Post Incident Analysis																	ü			

Appendix A: Detailed Mapping of MITS Mandatory Requirements and Microsoft Products and Services

Ref #	MITS Requirement	Microsoft Product/Service
Paragraph 9 - Roles and Responsibilities		
Paragraph 9.1 - IT Security Coordinator		
MR001	Departments must appoint an IT Security Coordinator with at least a functional reporting relationship to both the departmental Chief Information Officer and the Departmental Security Officer.	The IT Security Coordinator is a recipient of the security incident response information that Microsoft shares with Public Safety and Emergency Preparedness Canada (PSEPC) as part of the Security Cooperation Program (SCP). This information includes detailed update information and security-related metrics. For generic information regarding the SCP, see http://www.microsoft.com/industry/government/SCP.mspx.
MR002	The IT Security Coordinator must establish and manage a departmental IT security program as part of a coordinated departmental security program.	Microsoft offers a variety of risk assessment solutions, including solutions that analyze systems and suggest the most effective setup from a security standpoint. Microsoft also provides guidance that includes a methodology to assess and manage risk to IT systems. Specific guidance includes: • The Microsoft Security Risk Management Guide addresses how to identify assets and place a qualitative or quantitative value on each asset for the enterprise. For more information, see http://go.microsoft.com/fwlink/?linkid=30794. • Microsoft® Systems Management Server (SMS) provides many methods to control network security, including such capabilities as update and hotfix management, version management, network device discovery, and monitoring. For more information about SMS, see http://www.microsoft.com/smserver/default.mspx • For more information about how to use additional security methods to increase the security of your Microsoft Operations Manager (MOM) environment, see http://go.microsoft.com/fwlink/?linkid=33035. Systems Management Server (SMS) 2003 Desired Configuration Monitoring (DCM) is a powerful solution to monitor configuration settings across all server roles and hardware types for non-compliance. This helps identify undesired configuration changes that could result in security breaches or service disruptions. • For more information on the SMS 2003 DCM, see the Microsoft® Systems Management Server 2003 Desired Configuration Monitoring at http://www.microsoft.com/downloads/details.aspx?familyid=93A72AB8-BF54-4607-B9BB-AC9739C6C292&displaylang=en. In addition, the Microsoft® Management Server group works with partners to develop IT security and regulatory compliance solutions. Some of these partners have developed specific add-on service packs that audit key compliance controls for IT resources to support compliance governance efforts. These solutions provide event collection, alert templates, and reporting services to track auditing requirements for regulations, such as SOX, GLBA, and HIPAA.

		• For more information about partner solutions for MOM, see the Management Pack and Product Connector Catalog at http://www.microsoft.com/management/mma/catalog.aspx. Microsoft has also developed both a guide to help customers prevent vulnerabilities and a tool, the Microsoft® Baseline Security Analyzer (MBSA). The MBSA tool looks for common vulnerabilities and then notifies systems administrators to remediate them. • For more information about security monitoring and attack detection, see http://ww.microsoft.com/technet/security/topics/auditingandmonitoring/securitymonitoring/default.mspx. • For more information about the MBSA tool, see http://go.microsoft.com/fwlink/?linkid=10730. The Microsoft Security Assessment Tool provides small departments and agencies with a quick, high level view of their IT security readiness – see https://www.securityguidance.com/. The Microsoft Operations Framework (MOF) Self-Assessment tool can assist in improving your Microsoft operational environment. For additional information, see: http://www.microsoft.com/technet/itsolutions/cits/mo/mof/moftool.mspx . Additional guidelines with respect to systems hardening and security best practices are provided under MR006 below.
MR003	The IT Security Coordinator must review and recommend approval of departmental IT security policies and standards, and all policies that have IT security implications.	The Government Security Program provides access to the Windows source code (Client, Server) as well as the Office Suite, providing visibility into the standards that have been implemented within the product. The Government Systems Hardening Program (GSHP) provides draft versions of the security guidance to governments for their review and comment prior to publication. This provides the GoC with the ability to include its requirements in the commercial guidance that Microsoft publishes. By leveraging this process the GoC can significantly reduce the costs not only of publication but also of training and support for their environment since customized offerings for GoC specific guidance will not be required. Microsoft provides a wealth of security guidance, training and standards. For additional information, see: • Microsoft Home: http://www.microsoft.com/ • Security Related: http://www.microsoft.com/security • Product Related: http://www.microsoft.com/products • Partner resource: http://msreadiness.com/ • IT Pros: http://technet.microsoft.com/ • Developers: http://msdn.microsoft.com/ Additional guidance with respect to systems hardening and security

		best practices is provided under MR006.
MR004	The IT Security Coordinator must ensure review of the IT security related portions of Request for Proposals and other contracting documentation, including Security Requirements Checklists.	
MR005	The IT Security Coordinator must recommend approval of all contracts for external providers of IT security services.	
MR006	The IT Security Coordinator must work closely with program and service delivery managers to: • Ensure their IT Security needs are met, • Provide advice on safeguards, • Advise them of potential impacts of new and existing threats, and • Advise them on the residual risk of a program or service.	The Security Cooperation Program (SCP) provides the GoC with information regarding threats to Microsoft products. In addition, the Government Systems Hardening Program (GSHP) provides draft versions of the security guidance to governments for their review and comment prior to publication. This provides the GoC with the ability to include its requirements in the commercial guidance that Microsoft publishes. By harnessing this process the GoC can significantly reduce the costs not only of publication but also of training and support for their environment since customized offerings for GoC specific guidance will not be required. The Microsoft Threat Analysis & Modeling v2.0 tool (see http://msdn.microsoft.com/security/securecode/threatmodeling/acetm/) provides departments and agencies with the ability to review their planned and deployed environments to gain a better understanding of the safeguards that may be employed to manage business risk. Microsoft also provides a great deal of systems hardening guidance and security best practices to help secure various Microsoft products, including: Microsoft has developed the following guidance on basic host security: • For information about threats and countermeasures for Windows® XP and Windows Server® 2003, see the Threats and Countermeasures Guide at http://go.microsoft.com/fwlink/?linkid=15159. • For information about how to secure remote client and portable computers, see http://www.microsoft.com/technet/security/smallbusiness/topics/networksecurity/sec_remote_port_comp.mspx. • For information about the MBSA tool, see http://go.microsoft.com/fwlink/?linkid=10730. • For information about planning the security of services and service accounts, see

		http://www.microsoft.com/technet/security/topics/serversecurity/serviceaccount/default.mspx. Microsoft has developed the following guidance on host security: • For information about how to secure directory service administrative groups and accounts, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/activedirectory/sec_ad_admin_groups.mspx. • For information about how to secure Internet Information Services (IIS) versions 5.0 and 5.1, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/iis/sec_iis_5_0_5_1.mspx. • For information about how to secure IIS 6.0, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/iis/sec_iis_6_0.mspx. • For information about how to protect against network attacks, see http://www.microsoft.com/technet/security/smallbusiness/topics/networksecurity/prot_clients_net_attacks.mspx. • For information on Systems Management Server (SMS), see http://www.microsoft.com/technet/security/prodtech/SMS.mspx. • For information about security monitoring and attack detection, see The Security Monitoring and Attack Detection Planning Guide at http://www.microsoft.com/technet/security/topics/auditingandmonitoring/securitymonitoring/default.mspx. • For information about how to use SMS 2003 for patch management, see http://www.microsoft.com/technet/itsolutions/cits/mo/swdist/pmsms/2003/pmsms031.mspx. • For information on securing Microsoft Operations Manager, see the Microsoft Operations Manager 2005 Security Guide at http://www.microsoft.com/technet/prodtechnol/mom/mom2005/Library/3e039637-4639-46f7-9f5f-518e0c04795e.mspx?mfr=true. Microsoft has developed the following security guidance for Windows Server® 2003: • For information about security in Windows Server 2003, see Windows Server 2003 Security Guide at http://go.microsoft.com/fwlink/?linkid=14845. • For information about how to secure domain controllers in a Windows Server 2003 based network, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/windowsserver2003/sec_win2003_serv_dc.mspx. • For information about how to add and secure Windows Server 2003 in a Small Business Server 2003 Active Directory domain, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/windowsserver2003/win2k3sbnetwork.mspx. • For information about how to secure your Windows Small Business Server 2003–based network, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/sbs/sec_sbs2003_network.mspx. • For information about how to use Windows® Small Business Server 2003 to add and secure a computer running Windows® XP Professional, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/

		windowsxp/xp2sbs.mspx. • For information about Windows Server Update Services for Windows Server® 2003, see http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/wsus/default.mspx. Microsoft has developed the following guidance on Windows XP security: • For information about the features and recommended settings for Windows® XP with Service Pack 2 (SP2), see the Windows® XP Security Guide at http://go.microsoft.com/fwlink/?linkid=14839. • For information about how to secure Windows® XP Professional–based client computers in a Windows Server® environment, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/sec_winxp_pro_server_env.mspx. • For information about configuring Windows® XP with SP2 network protection technologies in an Active Directory environment, see http://www.microsoft.com/technet/security/prodtech/windowsxp/adprtect.mspx. • For information about configuring Windows® XP with SP2 network protection technologies in a small business environment, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/netprtct.mspx. • For information about configuring Windows® XP with SP2 network protection technologies on a single computer, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/protsing.mspx. • For information about configuring memory protection in Windows® XP with SP2, see http://www.microsoft.com/technet/security/prodtech/windowsxp/depcnfxp.mspx. • For information about how to secure Windows® XP Professional in a peer-to-peer environment, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/sec_winxp_pro_p2p.mspx. • For information about how to secure a Windows® XP Professional–based client computer in a Windows Server® 2003 Active Directory® domain, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/xpwinnet.mspx. Microsoft has developed the following guidance on Windows 2000 security: • For information about how to secure Windows® 2000 Server, see http://go.microsoft.com/fwlink/?linkid=14837. • For information about how to harden Windows® 2000, see the http://www.microsoft.com/technet/security/prodtech/windows2000/win2khg/01intro.mspx. • For information about how to secure Windows® 2000 domain controllers, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/windows2000/sec_win2000_serv_dc.mspx. Microsoft has developed the following guidance on Microsoft® Exchange Server: • For information about Exchange Server security and protection, see

		http://www.microsoft.com/technet/prodtechnol/exchange/2003/security.mspx. • For information about how to secure Exchange Server 2003, see Exchange Server 2003 Security Hardening Guide at http://go.microsoft.com/fwlink/?linkid=37804. • For information about improving message security, see Exchange Server 2003 Message Security Guide at http://go.microsoft.com/fwlink/?linkid=23216. Microsoft has developed the following guidance on Microsoft® Systems Management Server (SMS): • For information about established best practices to create the most secure SMS environment possible, see Scenarios and Procedures for Microsoft Systems Management Server 2003: Security at http://go.microsoft.com/fwlink/?linkid=31433. • For more information about SMS and its role in compliance, see the "Compliance Analysis" section of the Systems Management Server 2003 Operations Guide at http://www.microsoft.com/resources/documentation/sms/2003/all/opsguide/en-us/ops_3zoj.mspx. Microsoft has developed the following guidance on Microsoft® SQL Server: • For IT professional information regarding SQL Server 2005, see www.microsoft.com/technet/prodtechnol/sql/2005/default.mspx. • For developer information regarding SQL Server 2005, see http://msdn.microsoft.com/SQL/2005/default.aspx.
MR007	The IT Security Coordinator must monitor departmental compliance with this standard and associated documentation.	Microsoft offers several products that can help monitor compliance, including: • Microsoft® Baseline Security Analyzer (MBSA) tool see http://www.microsoft.com/technet/security/tools/mbsahome.mspx, • Microsoft® Operations Manager (MOM) – see http://www.microsoft.com/mom/evaluation/default.mspx • Systems Server Manager (SMS) – see http://www.microsoft.com/smserver/evaluation/default.mspx • Microsoft® Office Business Scorecard Manager - see http://office.microsoft.com/en-us/FX012225041033.aspx. • Systems Management Server (SMS) 2003 Desired Configuration Monitoring, see http://www.microsoft.com/downloads/details.aspx?familyid=93A72AB8-BF54-4607-B9BB-AC9739C6C292&displaylang=en.
MR008	The IT Security Coordinator must promote IT security in the department.	Microsoft provides a wealth of product independent security guidance, training and standards for a variety of audiences including IT Pros, Employees, Business users, and Developers. For additional information, see • Microsoft Home: http://www.microsoft.com/ • Security Related: http://www.microsoft.com/security • Product Related: http://www.microsoft.com/products • Partner resource: http://msreadiness.com/ • IT Pros: http://technet.microsoft.com/ • Developers: http://msdn.microsoft.com/

		In addition, Microsoft provides security education and awareness materials such as Public Service Announcements, Poster content, etc. – all provided at no cost for local reproduction via the Security Cooperation Program (SCP). Finally, Microsoft holds a variety of public security events including national security days, security summits, security seminars and youth summits on internet safety as part of our security mobilization program.
MR009	The IT Security Coordinator must establish an effective process to manage IT security incidents, and monitor compliance with it.	The following guidance from Microsoft is available on incident management and trouble-tracking: • For information about how to respond to IT security incidents, see www.microsoft.com/technet/security/topics/disasterrecovery/responding_sec_incidents.mspx. • For information about problem management, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfprbmg.mspx. • For information about incident management, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfincmg.mspx • For information about service desk functions, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfsvcdk.mspx • For more information about how to respond to incidents, see Windows Security Resource Kit Second Edition 2005, by Smith and Komar, from Microsoft Press. In addition, the next version of MOM (named System Center Operations Manager 2007) will include a security event audit feature for capturing and reporting on security events. To obtain additional information, see http://www.microsoft.com/mom/evaluation/beta/opsmgroverview.mspx. Furthermore, Microsoft supplies security incident data to PSEPC as part of the SCP, and this information is made available to IT Security Coordinators. Microsoft also implements a Software Security Incident Response Process (SSIRP) to provide prescriptive, authoritative guidance in support of incident management. Additional tools that can help monitor compliance are identified under MR007.
MR010	The IT Security Coordinator must serve as the department's principal IT security contact.	
MR011	The IT Security Coordinator position must be screened to the secret level or higher. In hiring for	

	this position, departments should give preference to individuals with appropriate professional certification.	
Paragraph 9.2 - Senior Management		
MR012	Senior management must address IT security requirements when defining the department's priorities, strategic directions, program objectives, budget and personnel allocations.	Microsoft offers a variety of software tools that can help senior management gather and present data that can inform and direct decisions about the alignment of IT spending and organizational strategies. Microsoft provides a guide that is intended to help decision makers assess and recommend information technology solutions designed to help collect and display information required to manage and measure the success of information technology projects. To download the guide, see http://download.microsoft.com/download/F/8/B/F8B274DB-814F-47E5-88C9-D57890BBFE7C/ESD_TDM_Guide.doc.
MR013	Senior management must also ensure adequate funding for security in IT projects, in accordance with Section 10.12 of the Government Security Policy.	See MR012.
MR014	Senior management must approve departmental IT security policies, standards and directives.	Microsoft actively participates in national and international standards bodies and implements these standards in our products.
Paragraph 9.3 - Departmental Security Officer		
MR015	Departments must appoint a Departmental Security Officer to establish and direct a departmental security program, and provide a list of their responsibilities.	
MR016	The Departmental Security Officer and the IT Security Coordinator must ensure that physical, personnel and IT security	Microsoft's IT Security strategy includes balanced, defence-in-depth measures (including people, processes, policies, products, and partnerships) to ensure a holistic and comprehensive approach to IT Security. Additional information is provided throughout this matrix.

	stakeholders coordinate their efforts to protect information and IT assets and ensure an integrated, balanced approach.	
Paragraph 9.4 – Chief Information Officer		
MR017	The department's Chief Information Officer is responsible for ensuring the effective and efficient management of the department's information and IT assets.	Microsoft produces guidance to help CIOs respond to this requirement, including the production of this MITS Compliance Guide.
MR018	The Chief Information Officer and the IT Security Coordinator must work together to ensure that appropriate security measures are applied to all departmental IM and IT assets, activities and processes.	Microsoft produces guidance to help CIOs respond to this requirement, including the production of this MITS Compliance Guide.
Paragraph 9.5 – Business Continuity Planning Coordinator		
MR019	The Chief Information Officer, Departmental Security Officer, IT Security Coordinator and the Business Continuity Planning Coordinator must work together to ensure a comprehensive approach to continuous service delivery.	Microsoft provides specific guidance on disaster recovery (also known as business continuity) and failover solutions. The following resources provide resources on backup and recovery: • Data Protection Manager (DPM) is the new Microsoft server software solution for rapid and reliable data recovery. For information about DPM, see http://www.microsoft.com/windowsserversystem/dpm/default.mspx • For information about Exchange Server Disaster Recovery Analyzer Tool V1.0, see http://www.microsoft.com/downloads/details.aspx?familyid=C86FA454-416C-4751-BD0E-5D945B8C107B&displaylang=en. • For general information about disaster recovery, see www.microsoft.com/technet/security/topics/disasterrecovery. • For information about how to back up and recover data, see www.microsoft.com/technet/security/smallbusiness/prodtech/windowsserver2003/backup_restore_data.mspx. • For information about how to back up and restore data from Windows Server® 2003, see www.microsoft.com/technet/security/smallbusiness/prodtech/windowsserver2003/ntbackup.mspx. • For information on backup and restore for Microsoft® Operations

		Manager, see http://www.microsoft.com/technet/prodtechnol/mom/mom2005/Library/4604e93a-31e1-43a3-b115-3c0e8c5a4dce.mspx. • For information on backup and restore for Systems Management Server, see http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops_5cis.mspx. • For information about how to back up and restore Windows® Small Business Server 2003, see www.microsoft.com/technet/security/smallbusiness/prodtech/sbs/backup_restore_sbs2003.mspx. • For a disaster recovery preparation worksheet for Exchange Server 2003, see http://www.microsoft.com/technet/prodtechnol/exchange/2003/drchecklist.mspx. • For information about SharePoint® Disaster Prevention and Recovery, see http://www.microsoft.com/technet/technetmag/issues/2005/11/BePrepared/default.aspx and http://www.microsoft.com/technet/prodtechnol/sppt/reskit/c2861881x.mspx. • For information about how to back up and restore data for Windows® 2000 Server, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/windows2000/backupwin2k.mspx. • For information about storage management, see http://www.microsoft.com/technet/itsolutions/cits/mo/smf/smfstomg.mspx. • For information about service continuity management, see http://www.microsoft.com/technet/itsolutions/cits/mo/smf/smfsrcmg.mspx. In addition, the following resources provide information about Microsoft components and solutions for redundancy: • For information about multi-master Active Directory, see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ad/ad/what_is_the_active_directory_replication_model.asp. • For information about SQL Server 2000 Failover Clustering, see www.microsoft.com/technet/prodtechnol/sql/2000/maintain/failclus.mspx. • For information about Server 2003 Network Load Balancing, see www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/nlb.mspx. • For information about Windows Server® 2003 cluster technology, see www.microsoft.com/windowsserver2003/technologies/clustering/default.mspx.
Paragraph 9.6 – Program and Service Delivery Managers		
MR020	On behalf of the department's Deputy Head, program and service delivery managers are	Microsoft's defence-in-depth strategy and security best practices guidance can help establish the appropriate level of security required in a given environment. Pointers to additional guidance in this area are provided under MR006.

	responsible for ensuring an appropriate level of security for their programs and services.	
MR021	In designing programs and services, managers will work with departmental security specialists to risk manage their programs or services.	Microsoft offers a variety of risk assessment solutions, including solutions that analyze systems and suggest the most effective setup from a security standpoint. Microsoft also provides guidance that includes a methodology to assess risk and manage risk to IT systems. Pointers to additional information with respect to risk management are provided under MR002.
MR022	Relying on the advice and support of the IT Security Coordinator, managers must determine the IT security requirements of their programs and services, have them accredited, and accept the associated residual risk.	Microsoft offers a variety of risk assessment solutions, including solutions that analyze systems and suggest the most effective setup from a security standpoint. Microsoft also provides guidance that includes a methodology to assess risk and manage risk for IT systems. Pointers to additional information with respect to risk management are provided under MR002.
MR023	Managers must ensure that, within their areas of responsibility, the requirements stated in this standard, the Government Security Policy and other related policies, standards and technical documentation, are met.	This Guide can assist managers in determining compliance with MITS. In addition, Microsoft provides several other tools that can help collect and display pertinent information, including: • Microsoft® Baseline Security Analyzer (MBSA) tool see http://www.microsoft.com/technet/security/tools/mbsahome.mspx, • Microsoft® Operations Manager (MOM) – see http://www.microsoft.com/mom/evaluation/default.mspx • Systems Server Manager (SMS) – see http://www.microsoft.com/smserver/evaluation/default.mspx • Microsoft® Office Business Scorecard Manager - see http://office.microsoft.com/en-us/FX012225041033.aspx.
Paragraph 9.7 – IT Operational Personnel		
MR024	IT operational personnel must follow security procedures and recommend improvements to them	Microsoft provides a wealth of information with respect to systems hardening and security best practices. Additional information is provided under MR006.
MR025	IT operational personnel must respond to security incidents.	The following guidance from Microsoft is available on incident management and trouble-tracking: • For information about how to respond to IT security incidents, see

		www.microsoft.com/technet/security/topics/disasterrecovery/responding_sec_incidents.mspx. • For information about problem management, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfprbmg.mspx. • For information about incident management, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfincmg.mspx • For information about service desk functions, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfsvcdk.mspx • For more information about how to respond to incidents, see Microsoft ®Windows® Security Resource Kit Second Edition 2005, by Smith and Komar, from Microsoft Press (see http://www.microsoft.com/MSPress/books/6815.asp) In addition, Microsoft supplies security incident data to PSEPC as part of the SCP, and this information is made available to IT Security Coordinators. Microsoft also implements a SSIRP to provide prescriptive, authoritative guidance in support of incident management.
MR026	IT operational personnel must test and install security patches.	Microsoft provides tools to help enterprise customers manage software updates and patches: • For information about how to use Systems Management Server 2003 for patch management, see http://www.microsoft.com/technet/itsolutions/cits/mo/swdist/pmsms/2003/pmsms031.mspx. • For information about Windows® Server Update Services (WSUS) for Windows Server® 2003, see www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/wsus/default.mspx.
MR027	IT operational personnel must maintain or upgrade security hardware and software.	Microsoft® Systems Management Server (SMS) provides many methods to control network security, including such capabilities as update and hotfix management, version management, network device discovery, and monitoring. For more information about SMS, see http://www.microsoft.com/smserver/default.mspx. Change management guidelines can be found at http://www.microsoft.com/technet/itsolutions/cits/mo/smf/smfchgmg.mspx. Microsoft provides prescriptive guidance and best practices for desktop deployment , including specific guidance related to security and patching. For additional information, see http://www.microsoft.com/technet/desktopdeployment/default.mspx and http://www.microsoft.com/technet/desktopdeployment/securitypatching/default.mspx. In addition, deployment guides for most Microsoft server-based products are available from the Microsoft® TechNet site (see http://www.microsoft.com/technet).
MR028	IT operational personnel must monitor systems and logs.	Microsoft offers several products that can help monitor systems and logs, including: • Microsoft® Baseline Security Analyzer (MBSA) tool see http://www.microsoft.com/technet/security/tools/mbsahome.mspx, • Microsoft® Operations Manager (MOM) – see

		http://www.microsoft.com/mom/evaluation/default.mspx • Systems Server Manager (SMS) – see http://www.microsoft.com/smserver/evaluation/default.mspx • Microsoft® Office Business Scorecard Manager - see http://office.microsoft.com/en-us/FX012225041033.aspx.
MR029	IT operational personnel must back up and recover information.	Refer to MR019.
MR030	IT operational personnel must manage access privileges and rights.	Much of the directory service within the Microsoft® Windows® 2000 Server and Windows Server® 2003 operating systems focuses on authentication, authorization, and access control. Internet Authentication Service (IAS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy. As a RADIUS server, IAS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless and virtual private network (VPN) connections. As a RADIUS proxy, IAS forwards authentication and accounting messages to other RADIUS servers. Microsoft provides the following general guidance on these access control solutions: • For information about securing administrator accounts, see The Administrator Accounts Security Planning Guide at www.microsoft.com/technet/security/topics/serversecurity/administratoraccounts/default.mspx • For information about how to select secure passwords, see Selecting Secure Passwords at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/select_sec_passwords.mspx. • For information about how to enforce strong password usage, see Enforcing Strong Password Usage Throughout Your Organization at www.microsoft.com/technet/security/smallbusiness/topics/networksecurity/enforce_strong_passwords.mspx. • For information about deploying and operating Public Key Infrastructure (PKI), see Deploying PKI Inside Microsoft at www.microsoft.com/technet/itsolutions/msit/security/deppkiin.mspx • For information about how to build an enterprise root certification authority in small and medium businesses, see Building an Enterprise Root Certification Authority in Small and Medium Businesses at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsserver2003/build_ent_root_ca.mspx. Microsoft provides the following specific examples on these access control solutions: • For information about using IAS, see Internet Authentication Service at www.microsoft.com/windowsserver2003/technologies/ias/default.mspx. • For information about how to use smart cards to secure access, see The Secure Access Using Smart Cards Planning Guide at

		www.microsoft.com/technet/security/topics/networksecurity/securesmartcards/default.mspx. • For information about using certificate services to secure wireless local area networks, see Securing Wireless LANs with Certificate Services at http://go.microsoft.com/fwlink/?linkid=14843. • For information about using Protected Extensible Authentication Protocol (PEAP) and passwords to secure wireless LANs, see Securing Wireless LANs with PEAP and Passwords at http://go.microsoft.com/fwlink/?linkid=23459. In addition, Role-Based Access Control (RBAC) is supported with Windows Server® 2003 Authorization Manager (AzMan). For additional information, see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetserv/html/AzManRoles.asp?_r=1. Furthermore, User Account Protection will be supported in Windows Vista, the next major release of the Windows® OS. This will isolate administration functions from general user functions. For additional information about Windows Vista™ security features, see http://www.microsoft.com/technet/windowsvista/evaluate/feat/secfeat.mspx. Additional information with respect to identity management is provided under MR084.
Paragraph 9.8 – Other Personnel		
MR031	All personnel must abide by the Government's and the department's IT security policy, procedures and other related documentation.	Microsoft believes that education and training is critical, and provides a variety of training (e.g., webcasts, security guidelines) and educational materials. Additional information can be found on-line at: • Microsoft Home: http://www.microsoft.com/ • Security Related: http://www.microsoft.com/security • Product Related: http://www.microsoft.com/products • Partner resource: http://msreadiness.com/ • IT Pros: http://technet.microsoft.com/ • Developers: http://msdn.microsoft.com/ In addition, Microsoft and its partners provide training solutions through the following resources that you can modify to meet the security and compliance requirements in this area for your organization: • For more information about Microsoft training, see http://www.microsoft.com/learning/training/default.asp. • For more information about Microsoft Office training, see http://office.microsoft.com/en-us/training/default.aspx. • For more information about workforce management, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfwrkmg.mspx.
MR032	All Personnel must report real and suspected security incidents to	Microsoft® Operations Manager (MOM) can send customize email notifications to individuals or a group of recipients based on alerts generated from selected security events. For additional information about MOM, see

	designated security officials, normally through their immediate supervisor.	http://www.microsoft.com/mom/evaluation/default.mspx. Incident management guidance can be found at http://www.microsoft.com/technet/itsolutions/cits/mo/smf/smfincmg.mspx. Additional information related to incident handling is provided under MR009. InfoPath is a tool that could be customized to collect data related to security incidents from GoC personnel. For additional information on InfoPath, see http://www.microsoft.com/office/infopath/prodinfo/overview.mspx.
Paragraph 9.9 – COMSEC Custodian		
MR033	Departments that hold classified cryptographic material, controlled cryptographic items or “accountable” publications require a COMSEC (Communications Security) account. These departments must appoint a COMSEC custodian (and an alternate, if required) to account for this material, items and publications in accordance with Communications Security Establishment instructions.	Microsoft provides several solutions for data classification and data protection. Windows® Rights Management Services (RMS) technologies allow you to both classify and protect the data in accordance with your organization’s security policy. RMS applies encryption-based, policy-driven protection that travels with the information wherever it goes. Additional data protection technology solution examples include Internet Protocol security (IPsec) and Encrypting File System (EFS). IPsec provides data integrity and encryption to IP traffic, whereas EFS encrypts files stored in the file systems of Microsoft® 2000, Windows® XP Professional, and Windows Server® 2003. Microsoft provides the following guidance on these data classification and protection solutions. • For more information about RMS, see http://www.microsoft.com/rms. • For more information about the information rights management capabilities of Office 2003, see http://www.microsoft.com/technet/prodtechnol/office/office2003/operate/of03irm.mspx. • For more information about Windows® Rights Management Services partner offerings, see http://www.microsoft.com/windowsserver2003/partners/rmspartners.mspx. • For information about IPsec, see http://www.microsoft.com/windowsserver2003/technologies/networking/ipsec/default.mspx. • For information about how to use IPsec and Group Policy to isolate servers and domains, see http://go.microsoft.com/fwlink/?linkid=33945. • For more information about EFS, see http://go.microsoft.com/fwlink/?linkid=46681. • For information about how to use EFS to protect data, see http://www.microsoft.com/technet/security/smallbusiness/topics/cryptographyetc/protect_data_efs.mspx. • For information about how to protect sensitive information from theft, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/efsxppro.mspx.

		In addition, full volume encryption will be supported in Windows Vista™ Enterprise Edition. The encryption algorithm used is AES-128 or AES-256. AES is endorsed by CSE. Microsoft will also offer pluggable crypto via the Crypto Next Generation (CNG) API and will also support Suite B cryptography (also endorsed by CSE). The Windows Vista Enterprise Edition will be available by the end of CY2006. For additional information regarding the security features that will be available with Vista, see http://www.microsoft.com/technet/windowsvista/evaluate/feat/secfeat.mspx.
Paragraph 9.10 – IT Project Managers		
MR034	IT project managers must ensure that project security requirements are met through the development and implementation of technical security specifications.	Microsoft embraces a defence-in-depth strategy and provides security best practices and product-specific security configuration advice. For additional information, see MR006.
Paragraph 10 – Departmental IT Security Policy		
MR035	Every department must have a department IT security policy based on the Government Security Policy, this standard and other related policies, standards and technical documentation. This policy can be a separate document or it can be policy statements within the departmental security policy. As a minimum, a departmental IT security policy must: • define the roles and responsibilities of program and service delivery managers, the	The Government Security Policy and MITS provide high-level guidance, and this MITS Compliance Guide can help GoC departments and agencies better understand how Microsoft products and services can address a majority of the mandatory requirements identified in MITS. Microsoft also provides guidance on security policy development. For additional information, see http://www.microsoft.com/technet/itsolutions/cits/mo/smf/mofsmsmf.mspx. Generic and product specific guidance available from Microsoft can also help. See MR006 for additional information. The Microsoft® Security Assessment Tool (MSAT) can also help smaller departments and agencies better understand their specific security requirements. For additional information on MSAT, see https://www.securityguidance.com/.

	Chief Information Officer, departmental legal, privacy specialists and security specialists, and other personnel with regard to IT security • make the necessary connections with other departmental policies, standards, and legal and regulatory requirements that relate to IT security (e.g., an acceptable use policy) • state the requirement for making IT security an integral part of program and service delivery • state a requirement for seeking funding in support of IT security requirements, • state requirements for the review and revision of the departmental IT security policy and supporting documentation.	
Paragraph 11 – IT Security Resources for Projects		
MR036	In planning new programs, services	Microsoft offers a wealth of prescriptive guidance and embraces a defence-in-depth IT Security strategy that can help in the planning

	or major upgrades to existing programs or services, the managers responsible must, at the earliest stage of the funding and approval process, determine the IT security requirements for these programs, services or upgrades and include resource requirements in funding requests.	process. See MR006 and MR037, as well as other information provided within this matrix.
Paragraph 12.1 – Management Controls		
Paragraph 12.1 – Security in the System Development Life Cycle		
MR037	Departments must address security and adjust security requirements throughout all the following stages of the system development life cycle, including at the earliest stages of planning and review: • Initiation — An initial Threat and Risk Assessment will provide input for IT security requirements. • Design and Development — An appropriate balance of technical, managerial, operational, physical and personnel security safeguards will help to meet the requirements determined by the Threat and	Microsoft has adopted a comprehensive defence-in-depth security strategy that includes security fundamentals (products that are secure by design and secure by default), as well as innovation to include a rich set of products with comprehensive security functionality. For information related to building secure applications, see: • For information about how to write secure code, see Writing Secure Code, Second Edition at http://www.microsoft.com/mspress/books/5957.asp. • For information about how security fits into the software development life cycle, see The Trustworthy Computing Security Development Lifecycle at http://msdn.microsoft.com/security/sdl. • For information about how to develop secure applications, see http://www.microsoft.com/technet/security/topics/DevSecApps.mspx. • For information about building secure ASP.NET applications, see Building Secure ASP.NET Applications: Authentication, Authorization, and Secure Communication at http://www.msdn.microsoft.com/library/en-us/dnnetsec/html/secnetlpMSDN.asp. • For more information about how to improve Web application security, see Improving Web Application Security: Threats and Countermeasures at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/ThreatCounter.asp. • For more information regarding threat modeling, see http://msdn.microsoft.com/security/securecode/threatmodeling/default.aspx. For additional generic information, see: • For information about the NIST SP 800 series of best practice guides, see NIST Special Publications SP 800 Series at http://csrc.nist.gov/publications/nistpubs/. • For information about software security, see the 19 Deadly Sins of

	Risk Assessment. • Implementation — Design documentation, acceptance tests, and certification and accreditation are to be performed. • Operation — System security is monitored and maintained while Threat and Risk Assessments aid in the evaluation of modifications that could affect security. • Disposal — In accordance with archival and security standards and guidelines, archive or dispose of sensitive IT assets and information resident on the system.	Software Security at http://www.books.mcgraw-hill.com/getbook.php?isbn=0072260858. Microsoft also offers tools and guidance with respect to risk management. For additional information, see MR002. Microsoft also offers prescriptive guidance with respect to systems hardening and security best practices. For additional information, see MR006.
Paragraph 12.2 – Identification and Categorization of Information and IT Assets		
MR038	Departments must determine the criticality and sensitivity of their information and IT assets with regard to confidentiality, integrity, availability and value.	Microsoft provides threat modeling tools that can assist in meeting this requirement. For more information regarding threat modeling, see http://msdn.microsoft.com/security/securecode/threatmodeling/default.aspx.
Paragraph 12.3 – Security Risk Management		
MR039	Departments must continuously manage the security risks of information and IT assets throughout the life of their programs and services. Security risk management activities include:	Microsoft offers a variety of risk assessment solutions, including solutions that analyze systems and suggest the most effective setup from a security standpoint. Microsoft also provides guidance that includes a methodology to assess risk and manage risk to IT systems. • The Microsoft Security Risk Management Guide addresses how to identify assets and place a qualitative or quantitative value on each asset for the enterprise. For more information, see http://go.microsoft.com/fwlink/?linkid=30794. • Risk Management is a core discipline of the Microsoft Solutions Framework (MSF). MSF recognizes that change and the resulting

	Threat and Risk Assessments, audits, Business Impact Analysis, Privacy Impact Assessments, self-assessments, monitoring, security investigations, and Vulnerability Assessments.	uncertainty are inherent aspects of the IT lifecycle. For more information on the MSF Risk Management Discipline, see http://www.microsoft.com/downloads/details.aspx?FamilyID=6c2f2c7e-ddbd-448c-a218-074d88240942&DisplayLang=en. • The Microsoft Operations Framework Risk Management Discipline for Operations is available at http://www.microsoft.com/technet/itsolutions/cits/mo/mof/mofrisk.mspx. • Microsoft® Systems Management Server (SMS) provides many methods to control network security, including such capabilities as update and hotfix management, version management, network device discovery, and monitoring. For more information about SMS, see http://www.microsoft.com/smserver/default.mspx. • For more information about how to use additional security methods to increase the security of your Microsoft® Operations Manager (MOM) environment, see http://go.microsoft.com/fwlink/?linkid=33035. Microsoft has also developed both a guide to help customers prevent vulnerabilities and a tool, the Microsoft® Baseline Security Analyzer (MBSA). The MBSA tool looks for common vulnerabilities and then notifies systems administrators to remediate them. • For more information about security monitoring and attack detection, see www.microsoft.com/technet/security/topics/auditingandmonitoring/securitymonitoring/default.mspx. • For more information about the MBSA tool, see http://go.microsoft.com/fwlink/?linkid=10730. Other Microsoft products that can help in the management and assessment area include: • Microsoft® Operations Manager (MOM) – see http://www.microsoft.com/mom/evaluation/default.mspx • Microsoft® Systems Server Manager (SMS) – see http://www.microsoft.com/smserver/evaluation/default.mspx • Microsoft® Office Business Scorecard Manager - see http://office.microsoft.com/en-us/FX012225041033.aspx. The Microsoft® Security Assessment Tool (MSAT) provides small departments and agencies with a quick, high level view of their IT security readiness – see https://www.securityguidance.com/. The Microsoft® Operations Framework (MOF) Self-Assessment tool can assist in improving your Microsoft operational environment. For additional information, see: http://www.microsoft.com/technet/itsolutions/cits/mo/mof/moftool.mspx In addition, Microsoft has developed several change management solutions, including: • Microsoft provides guidance for IT professionals on the basics of change management, which you also can apply to compliance. This guidance appears in the Service Management Functions (SMFs) series. For more information about change management,

		see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfchgmg.mspx. • Microsoft® SharePoint® Services works with partner solutions to provide an example of how to control change in IT systems. For more information, see the Windows® SharePoint® Services Applications Template: Change Management at www.microsoft.com/downloads/details.aspx?FamilyId=8481322A-88EA-44CF-9DB2-63B43A03FEB2&displaylang=en. • The Microsoft Office Solution Accelerator for Sarbanes-Oxley demonstrates the capability of Microsoft Office to manage the process of attaining compliance with the regulations in this act. For more information about this solution, see the Office Solution Accelerator for Sarbanes-Oxley site at http://msdn.microsoft.com/office/understanding/SOX/default.aspx. • For information about Microsoft® Systems Management Server, which manages change on clients and servers, see www.microsoft.com/technet/security/prodtech/SMS.mspx. • Microsoft has also worked with partners to create change management solutions using Microsoft Office. For more information about such partner solutions, contact your local Microsoft sales office.
Paragraph 12.3.2 – Threat and Risk Assessment		
MR040	Departments must apply security measures above baseline levels when justified by a Threat and Risk Assessment.	Microsoft offers a variety of risk assessment solutions, including solutions that analyze systems and suggest the most effective setup from a security standpoint. Microsoft also provides guidance that includes a methodology to assess and manage risk to IT systems. Pointers to additional information with respect to risk management are provided under MR002.
MR041	Departments must conduct a Threat and Risk Assessment for every program, system or service. Threat and Risk Assessments can be short and simple or far more detailed and rigorous, depending on the sensitivity, criticality and complexity of the program, system or service being assessed.	Microsoft offers a variety of risk assessment solutions, including solutions that analyze systems and suggest the most effective setup from a security standpoint. Microsoft also provides guidance that includes a methodology to assess and manage risk to IT systems. Pointers to additional information with respect to risk management are provided under MR002.
Paragraph 12.3.3 – Certification and Accreditation		
MR042	Departments must have their systems or services certified and accredited before approving them for operation.	A number of Microsoft's products have achieved Common Criteria (CC) certification. For example, the following products were certificate EAL4+ in November 2005: • Microsoft® Windows® Server 2003, Standard Edition; SP 1 • Microsoft® Windows® Server 2003, Enterprise Edition; SP 1 • Microsoft® Windows® Server 2003, Datacenter Edition; SP 1

	The graduated performance of certification depends upon the quantity and quality of certification evidence required by the accreditation authority. Such evidence can include the results of any applicable Threat and Risk Assessment, a Business Impact Assessment, a Privacy Impact Assessment, a Vulnerability Assessment, security tests and product evaluation, self-assessments, audits and security reviews and related legal or policy assessments that demonstrate conformance to relevant legislation or policy.	• Microsoft® Windows Server® 2003 Certificate Server, Certificate Issuing and Management Components (CIMC) (Security Level 3 Protection Profile, Version 1.0) • Microsoft® Windows® XP, Professional; SP 2 • Microsoft® Windows® XP, Embedded; SP 2 • Additional evaluations prior to November 2005 include: • Microsoft® ISA Server 2004 SE (EAL4, September 2005) • Microsoft® Exchange Server 2003 (EAL4, November 2005) • Microsoft® Windows® 2000 Professional, Windows Server® and Advanced Server (EAL4+, Oct 2003)
MR043	Departments must periodically review the accreditation of systems or services if the systems or services have changed significantly or if warranted due to changes in the risk environment. *NOTE: For common systems or services, the Government of Canada Chief Information Officer is the accreditation authority. For systems or services that are specific to a department, the program or service delivery manager is responsible for accreditation. For	Microsoft has developed several change management solutions, including: • Microsoft provides guidance for IT professionals on the basics of change management, which you also can apply to compliance. This guidance appears in Service Management Functions (SMFs) series. For more information about change management, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfchgmg.mspx. • Microsoft® SharePoint® Services works with partner solutions to provide an example of how to control change in IT systems. For more information, see the Windows SharePoint Services Applications Template: Change Management at www.microsoft.com/downloads/details.aspx?FamilyId=8481322A-88EA-44CF-9DB2-63B43A03FEB2&displaylang=en. • The Microsoft Office Solution Accelerator for Sarbanes-Oxley demonstrates the capability of Microsoft Office to manage the process of attaining compliance with the regulations in this act. For more information about this solution, see the Office Solution Accelerator for Sarbanes-Oxley site at http://msdn.microsoft.com/office/understanding/SOX/default.aspx. • For information about Microsoft® Systems Management Server, which manages change on clients and servers, see www.microsoft.com/technet/security/prodtech/SMS.mspx. • Microsoft has also worked with partners to create change management solutions using Microsoft Office. For more

	systems or services shared by two or more organizations, the manager of the program or service is the accreditation authority	information about such partner solutions, contact your local Microsoft sales office.
Paragraph 12.5 – Vulnerability Management		
MR044	Departments must continuously manage vulnerabilities for their programs, systems and services. This management task includes the discovery of vulnerabilities, and the implementation of corresponding solutions. As part of discovery, departments must actively review sources of vulnerability information to determine the potential affect on their programs, systems and services.	Microsoft offers several products that can help continuously monitor systems, including: • Microsoft® Baseline Security Analyzer (MBSA) tool see http://www.microsoft.com/technet/security/tools/mbsahome.mspx, • Microsoft® Operations Manager (MOM) – see http://www.microsoft.com/mom/evaluation/default.mspx • Systems Server Manager (SMS) – see http://www.microsoft.com/smserver/evaluation/default.mspx • Microsoft® Office Business Scorecard Manager - see http://office.microsoft.com/en-us/FX012225041033.aspx. Systems Management Server (SMS) 2003 Desired Configuration Monitoring (DCM) is a powerful solution to monitor configuration settings across all server roles and hardware types for non-compliance. This helps identify undesired configuration changes that could result in security breaches or service disruptions. For more information on the SMS 2003 DCM, see the Microsoft® Systems Management Server 2003 Desired Configuration Monitoring at http://www.microsoft.com/downloads/details.aspx?familyid=93A72AB8-BF54-4607-B9BB-AC9739C6C292&displaylang=en. Microsoft also has produced a security monitoring and attack detection guide for security professionals that provides information on the detection and monitoring process. For more information, see The Security Monitoring and Attack Detection Planning Guide at http://www.microsoft.com/technet/security/topics/auditingandmonitoring/securitymonitoring/default.mspx. The Microsoft® Security Assessment Tool (MSAT) can also help smaller departments and agencies better understand their specific security requirements. For additional information on MSAT, see https://www.securityguidance.com/ The Microsoft® Threat Analysis & Modeling v2.0 tool (see http://msdn.microsoft.com/security/securecode/threatmodeling/acetm/) provides departments and agencies with the ability to review their planned and deployed environments to gain a better understanding of the security safeguards that may be employed to manage business risk. Pointers to additional information related to risk management are provided under MR002.
MR045	As part of solution management, departments must determine the risk	Pointers to information regarding risk management are provided under MR002. In addition, Microsoft provides tools to help enterprise customers manage software updates and patches, including:

	posed by vulnerabilities. Based upon this risk, departments should test the impact of the proposed solution to the vulnerability, and subsequently implement and deploy the solution (e.g. software patch).	• For information about how to use Systems Management Server 2003 for patch management, see http://www.microsoft.com/technet/itsolutions/cits/mo/swdist/pmsms/2003/pmsms031.mspx. • For information about Windows® Server Update Services (WSUS) for Windows Server® 2003, see www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/wsus/default.mspx.
Paragraph 12.5.1 – Vulnerability Assessments		
MR046	Departments must conduct a vulnerability assessment regularly on highly sensitive or highly exposed systems, and on a discretionary basis on other systems.	Pointers to information regarding risk management are provided under MR002.
MR047	Departments must document vulnerability assessments, subsequent decisions and remedial actions, e.g. software patches.	Pointers to information regarding risk management are provided under MR002. In addition, Microsoft provides tools to help enterprise customers manage software updates and patches, including: • For information about how to use Systems Management Server 2003 for patch management, see http://www.microsoft.com/technet/itsolutions/cits/mo/swdist/pmsms/2003/pmsms031.mspx. • For information about Windows® Server Update Services (WSUS) for Windows Server® 2003, see www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/wsus/default.mspx.
Paragraph 12.5.2 – Patch Management		
MR048	Departments must establish a systematic, documented patch management process to ensure they apply security-related patches in a timely manner. The IT Security Coordinator must ensure that this process is effective and that the department follows it	Microsoft provides tools to help enterprise customers manage software updates and patches, including: • For information about how to use Systems Management Server 2003 for patch management, see http://www.microsoft.com/technet/itsolutions/cits/mo/swdist/pmsms/2003/pmsms031.mspx. • For information about Windows® Server Update Services (WSUS) for Windows Server® 2003, see www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/wsus/default.mspx. In addition, an overview of the patch management process can be found at http://www.microsoft.com/technet/security/topics/patchmanagement/secmod193.mspx.

Paragraph 12.6 – Segregation of Responsibilities		
MR049	Departments must segregate IT responsibilities as much as possible.	Role-Based Access Control (RBAC) is supported with Windows Server® 2003 Authorization Manager (AzMan). For additional information, see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetserv/html/AzManRoles.asp?_r=1. Furthermore, User Account Protection will be supported in Windows Vista™, the next major release of the Windows® OS. This will isolate administration functions from general user functions. For additional information about Windows Vista security features, see http://www.microsoft.com/technet/windowsvista/evaluate/feat/secfeat.mspx. Additional information with respect to identity management is provided under MR084.
MR050	Individuals who are authorized to conduct sensitive operations must not be allowed to audit these operations.	Role-Based Access Control (RBAC) is supported with Windows Server® 2003 Authorization Manager (AzMan). For additional information, see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetserv/html/AzManRoles.asp?_r=1. Furthermore, User Account Protection will be supported in Windows Vista™, the next major release of the Windows® OS. This will isolate administration functions from general user functions. For additional information about Windows Vista security features, see http://www.microsoft.com/technet/windowsvista/evaluate/feat/secfeat.mspx. Additional information with respect to identity management is provided under MR084.
Paragraph 12.7 – Contracting		
MR051	Before issuing a contract, departments must ascertain if IT security is relevant to the goods or services to be provided by the contractor, and if so, account for the security requirements at every stage of contracting.	
MR052	Departments must identify individuals within the	

	department to oversee the work of external IT security service providers.	
Paragraph 12.8 – Continuity Planning		
MR053	As part of their business continuity planning, departments must produce and routinely test and revise an IM continuity plan and an IT continuity plan.	See MR019.
MR054	The Business Continuity Planning Coordinator must collaborate with the IT Security Coordinator throughout business continuity planning	
Paragraph 12.9 – Sanctions		
MR055	Departments (must) apply sanctions (in response) to IT security incidents when in the opinion of the deputy head there has been misconduct or negligence.	
Paragraph 12.10 – Sharing and Exchange of Information and IT Assets		
MR056	Departments that share information, IT infrastructure or other IT assets must establish a written security arrangement that defines the terms and conditions of any authorized sharing, and recognize any legal impediments to the sharing.	Microsoft shares incident and vulnerability information with PSEPC via the Security Cooperation Program (SCP), and this information is shared with other GoC departments and agencies. Microsoft also provides technologies that can support policy-based labels and enforce access restrictions to information as it flows from one department to another. Windows® Rights Management Services (RMS) technologies allow you to both label and protect your data based on organizational security policy. RMS applies encryption-based, policy-driven protection that travels with the information wherever it goes. For more information about RMS, see http://www.microsoft.com/rms.
MR057	Departments that share information or other assets or use common	Use of Microsoft products such as RMS (see MR056) can help to ensure common implementation across the GoC. Additional information related to information protection and cryptography is

	infrastructure must conform to the security standards defined for that system or infrastructure.	provided under MR090.
MR058	Departments that hold or use information from outside the Government of Canada (e.g., from industry, provincial government, or international parties) must respect existing agreements or arrangements with the parties that have provided the information.	See MR056 and MR057.
Paragraph 12.11 – Departmental IT Security Assessment and Audit		
MR059	Departments need to actively monitor their management practices and controls. As part of this responsibility, departments assess and audit IT security and remedy deficiencies where necessary.	See MR002.
Paragraph 12.11.1 – Self-Assessment		
MR060	Departments must conduct an annual assessment of their IT security program and practices to monitor compliance with government and departmental security policies and standards using the IT Security Self-Assessment methodology developed by the Treasury Board Secretariat.	See MR002.
MR061	Based on the results of this self-	See MR002.

	assessment, departments must develop or update their IT security action plan and determine the resources required to implement it.	
MR062	Departments must submit their IT Security Self-Assessment whenever the Government's Chief Information Officer requests it to help Treasury Board Secretariat assess the state of security across government.	See MR002.
Paragraph 12.11.2 – Internal Audit		
MR063	Planning for IT security audits must be incorporated into the overall departmental internal audit planning process, and prioritized in accordance with the TBS Policy on Internal Audit, departmental and Government of Canada requirements and the overall departmental risk management strategy and practices	See MR002.
MR064	The IT Security Coordinator and the Chief Information Officer must be consulted during each phase of any audit of the IT security program, and in all audits of departmental programs or services that have	See MR002.

	an IT security component	
Paragraph 12.12 – IT Security Awareness		
MR065	Departments must inform and regularly remind personnel of IT security responsibilities, concerns and issues.	Microsoft believes that education and training is critical, and we provide a variety of training (e.g., webcasts, security guidelines) and educational materials. Additional information can be found on-line at: • Microsoft Home: http://www.microsoft.com/ • Security Related: http://www.microsoft.com/security • Product Related: http://www.microsoft.com/products • Partner resource: http://msreadiness.com/ • IT Pros: http://technet.microsoft.com/ • Developers: http://msdn.microsoft.com/ In addition, Microsoft and its partners provide training solutions through the following resources that you can modify to meet the security and compliance requirements in this area for your organization: • For more information about Microsoft training, see http://www.microsoft.com/learning/training/default.asp. • For more information about Microsoft Office training, see http://office.microsoft.com/en-us/training/default.aspx. • For more information about workforce management, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfwrkmg.mspx.
MR066	Departments must provide IT security awareness in their employee orientation training.	Microsoft believes that education and training is critical, and provides a variety of training (e.g., webcasts, security guidelines) and educational materials. Additional information can be found on-line at: • Microsoft Home: http://www.microsoft.com/ • Security Related: http://www.microsoft.com/security • Product Related: http://www.microsoft.com/products • Partner resource: http://msreadiness.com/ • IT Pros: http://technet.microsoft.com/ • Developers: http://msdn.microsoft.com/ In addition, Microsoft and its partners provide training solutions through the following resources that you can modify to meet the security and compliance requirements in this area for your organization: • For more information about Microsoft training, see http://www.microsoft.com/learning/training/default.asp. • For more information about Microsoft Office training, see http://office.microsoft.com/en-us/training/default.aspx. • For more information about workforce management, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfwrkmg.mspx.
MR067	Departments must ensure that all personnel know of the security risks associated with computers at workstations and	Microsoft believes that education and training is critical, and provides a variety of training (e.g., webcasts, security guidelines) and educational materials. Additional information can be found on-line at: • Microsoft Home: http://www.microsoft.com/ • Security Related: http://www.microsoft.com/security • Product Related: http://www.microsoft.com/products

	other equipment (e.g. Personal Digital Assistants - PDAs), given that the security of the information accessed depends primarily on the person using the equipment.	• Partner resource: http://msreadiness.com/ • IT Pros: http://technet.microsoft.com/ • Developers: http://msdn.microsoft.com/ In addition, Microsoft and its partners provide training solutions through the following resources that you can modify to meet the security and compliance requirements in this area for your organization: • For more information about Microsoft training, see http://www.microsoft.com/learning/training/default.asp. • For more information about Microsoft Office training, see http://office.microsoft.com/en-us/training/default.aspx. • For more information about workforce management, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfwrkmg.mspx. Microsoft also provides product-specific guidance on systems hardening and security best practices as identified under MR006 and elsewhere within this matrix.
Paragraph 12.13 – IT Security Training		
MR068	Departments must provide ongoing IT security training to all individuals with significant IT security responsibilities.	Microsoft believes that education and training is critical, and provides a variety of training (e.g., webcasts, security guidelines) and educational materials. Additional information can be found on-line at: • Microsoft Home: http://www.microsoft.com/ • Security Related: http://www.microsoft.com/security • Product Related: http://www.microsoft.com/products • Partner resource: http://msreadiness.com/ • IT Pros: http://technet.microsoft.com/ • Developers: http://msdn.microsoft.com/ In addition, Microsoft and its partners provide training solutions through the following resources that you can modify to meet the security and compliance requirements in this area for your organization: • For more information about Microsoft training, see http://www.microsoft.com/learning/training/default.asp. • For more information about Microsoft Office training, see http://office.microsoft.com/en-us/training/default.aspx. • For more information about workforce management, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfwrkmg.mspx.
Paragraph 13 – Graduated Safeguards		
MR069	Departments must apply graduated safeguards that are commensurate with the risks to their information and IT assets, with more rigorous safeguards as asset values, service delivery	Microsoft embraces a defence-in-depth strategy that helps organizations deploy security products to protect against the identified threats; and the configuration of specific products can be customized in accordance with the security policy and associated risk assessment associated with a particular environment. Where appropriate, the security of specific products can also be enhanced through the use of additional safeguards (e.g., two-factor authentication versus one-factor authentication). Additional product-specific information is identified under MR006 and

	requirements and threats to confidentiality, availability or integrity increase.	elsewhere within this matrix.
Paragraph 14.1 – Configuration Management and Change Control		
MR070	When proposing configuration management or system changes, departments must seek the advice of the IT Security Coordinator where changes could potentially compromise security.	Microsoft has developed several change management/change control solutions, including: • Microsoft provides guidance for IT professionals on the basics of change management, which you also can apply to compliance. This guidance appears in the Service Management Functions (SMFs) series. For more information about change management, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfchgmg.mspx. • Microsoft® SharePoint® Services works with partner solutions to provide an example of how to control change in IT systems. For more information, see the Windows® SharePoint® Services Applications Template: Change Management at www.microsoft.com/downloads/details.aspx?FamilyId=8481322A-88EA-44CF-9DB2-63B43A03FEB2&displaylang=en. • The Microsoft® Office Solution Accelerator for Sarbanes-Oxley demonstrates the capability of Microsoft® Office to manage the process of attaining compliance with the regulations in this act. For more information about this solution, see the Office Solution Accelerator for Sarbanes-Oxley site at http://msdn.microsoft.com/office/understanding/SOX/default.aspx. • For information about Microsoft® Systems Management Server, which manages change on clients and servers, see www.microsoft.com/technet/security/prodtech/SMS.mspx. • Microsoft has also worked with partners to create change management solutions using Microsoft® Office. For more information about such partner solutions, contact your local Microsoft sales office.
Paragraph 14.2 – Problem Reporting/Help Desk		
MR071	IT security measures must be incorporated into the routine functions of the Department's problem reporting process or centralized Help Desk facility	The following guidance from Microsoft is available on incident management, trouble-tracking and reporting: • For information about how to respond to IT security incidents, see www.microsoft.com/technet/security/topics/disasterrecovery/responding_sec_incidents.mspx. • For information about problem management, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfprbmg.mspx. • For information about incident management, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfincmg.mspx. • For information about service desk functions, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfsvcdk.mspx. • For more information about how to respond to incidents, see Microsoft® Windows® Security Resource Kit Second Edition 2005, by Smith and Komar, from Microsoft Press. See

		http://www.microsoft.com/MSPress/books/6815.asp Microsoft provides a solution accelerator for auto-ticketing for organizations that have deployed (or are considering deploying) MOM 2005. For more information, see Autoticketing Solution Accelerator at http://www.microsoft.com/technet/itsolutions/cits/mo/smc/as05.mspx. For information on automatically creating tickets in 3rd party Service Desk products based on alerts received within MOM, see Microsoft Operations Manager Product Connectors at http://www.microsoft.com/management/momprodconnectors.mspx. In addition, Microsoft supplies security incident data to PSEPC as part of the SCP, and this information is made available to IT Security Coordinators. Microsoft also implements a SSIRP to provide prescriptive, authoritative guidance in support of incident management.
MR072	Where the incident involves a possible security breach, documented response procedures must outline how Help Desk personnel will document the event, identify trends, notify the IT Security Coordinator or an incident response team, and instruct the user on how to proceed.	The following guidance from Microsoft is available on incident management and trouble-tracking: • For information about how to respond to IT security incidents, see www.microsoft.com/technet/security/topics/disasterrecovery/responding_sec_incidents.mspx. • For information about problem management, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfprbmg.mspx. • For information about incident management, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfincmg.mspx • For information about service desk functions, see www.microsoft.com/technet/itsolutions/cits/mo/smf/smfsvcdk.mspx • For more information about how to respond to incidents, see Microsoft® Windows® Security Resource Kit Second Edition 2005, by Smith and Komar, from Microsoft Press. Microsoft provides a solution accelerator for auto-ticketing for organizations that have deployed (or are considering deploying) MOM 2005. For more information, see Autoticketing Solution Accelerator at http://www.microsoft.com/technet/itsolutions/cits/mo/smc/as05.mspx. For information on automatically creating tickets in 3rd party Service Desk products based on alerts received within MOM, see Microsoft Operations Manager Product Connectors at http://www.microsoft.com/management/momprodconnectors.mspx. In addition, Microsoft supplies security incident data to PSEPC as part of the SCP, and this information is made available to IT Security Coordinators. Microsoft also implements a Software Security Incident Response Process (SSIRP) to provide prescriptive, authoritative guidance in support of incident management.
Paragraph 14.4 – System Support Services		
MR073	Departments must ensure that underlying system	Microsoft provides a number of underlying tools to support this requirement, including audit and logging tools in support of event tracking, including:

	services (e.g. trusted time, event logging) are provided to support security services.	• Microsoft® Baseline Security Analyzer (MBSA) tool see http://www.microsoft.com/technet/security/tools/mbsahome.mspx, • Microsoft® Operations Manager (MOM) – see http://www.microsoft.com/mom/evaluation/default.mspx • Systems Server Manager (SMS) – see http://www.microsoft.com/smserver/evaluation/default.mspx • Microsoft® Office Business Scorecard Manager - see http://office.microsoft.com/en-us/FX012225041033.aspx.
Paragraph 15 – Active Defence Strategy		
MR074	Departments must adopt an active defence strategy that includes prevention, detection, response and recovery (PDRR)	Microsoft has adopted a comprehensive defence-in-depth security strategy that includes security fundamentals (products that are secure by design and secure by default), as well as innovation to include a rich set of products with comprehensive security functionality. Prevention includes secure software by design (SDLC, threat modeling) and secure by default (systems hardening guidance). Critical and Internet-facing software undergoes a rigorous Software Development Life Cycle (SDLC) process, see http://msdn.microsoft.com/security/default.aspx?pull=/library/en-us/dnsecure/html/sdl.asp and includes threat modeling, see http://msdn.microsoft.com/security/securecode/threatmodeling/default.aspx. Microsoft also publishes a variety of product-specific systems hardening guides, many of these developed in cooperation with national governments. The Government Systems Hardening Program (GSHP) provides draft versions of the security guidance to governments for their review and comment prior to publication. This provides the GoC with the ability to include its requirements in the commercial guidance that Microsoft publishes. By leveraging this process the GoC can significantly reduce the costs not only of publication but also of training and support for their environment since customized offerings for GoC specific guidance will not be required. Pointers to additional information are provided under MR006 and elsewhere in this matrix. In addition, the Government Security Program provides access to the Windows source code (Client, Server) as well as the Office Suite, affording governments an opportunity to review source code developed by Microsoft. The GoC is a participant in the Government Security Program. Furthermore, a number of Microsoft's products have achieved Common Criteria (CC) certification which provides even more assurance that the software implements the expected functionality. For example, the following products were certificate EAL4+ in November 2005: • Microsoft® Windows® Server 2003, Standard Edition; SP 1 • Microsoft® Windows® Server 2003, Enterprise Edition; SP 1 • Microsoft® Windows® Server 2003, Datacenter Edition; SP 1 • Microsoft® Windows® Server 2003 Certificate Server, Certificate Issuing and Management Components (CIMC) (Security Level 3 Protection Profile, Version 1.0) • Microsoft® Windows® XP, Professional; SP 2

		• Microsoft® Windows® XP, Embedded; SP 2 Additional evaluations prior to November 2005 include: • Microsoft® ISA Server 2004 SE (EAL4, September 2005) • Microsoft® Exchange Server 2003 (EAL4, November 2005) • Microsoft® Windows® 2000 Professional, Windows Server and Advanced Server (EAL4+, Oct 2003) Finally, Microsoft offers Risk Assessment tools that can help develop an active defence strategy. Some of these tools are identified under MR002. Additional specifics regarding detection, response and recovery are provided further below.
MR075	Departments must continuously monitor threats and vulnerabilities and, where required, take proactive countermeasures.	Through the Security Cooperation Program (SCP), Microsoft shares up-to-date information regarding threats and vulnerabilities related to Microsoft products, including recommendations for taking proactive measures to fix any known vulnerabilities. Departmental IT Security Coordinators are recipients of this information. For generic information regarding the SCP, see http://www.microsoft.com/industry/government/SCP.mspx. Additional information related to risk assessment is provided under MR002.
MR076	Departments must take action in response to alerts and advisories from Public Safety and Emergency Preparedness Canada (PSEPC), and consider information from security vendors and external surveillance bodies such as the Computer Emergency Response Team Coordination Center (CERT CC).	Through the Security Cooperation Program (SCP), Microsoft shares alerts and advisories directly with PSEPC. Departmental IT Security Coordinators are recipients of this information. For generic information regarding the SCP, see http://www.microsoft.com/industry/government/SCP.mspx. Additional information related to incident handling is provided under MR009.
MR077	During increased Readiness Levels or periods of heightened IT threat, departments are required to increase their vigilance by, for	Through the SCP, Microsoft shares incident information with the GoC on an ongoing basis, including during times of crisis. For generic information regarding the SCP, see http://www.microsoft.com/industry/government/SCP.mspx.

	example, increasing the operating hours of a departmental Information Protection Centre (IPC) to twenty-four hours a day, seven days a week.	
Paragraph 16.1 – Physical Security within the IT Security Environment		
MR078	Departments must protect portable devices such as laptops, handheld digital devices and cell phones, given the information they contain and their monetary value.	Microsoft offers technologies that can protect information in the event a device such as a laptop or a Pocket PC is stolen: • For information about full volume encryption available with Windows Vista™ Enterprise (to be available in Q4 CY2006), see http://www.microsoft.com/technet/windowsvista/library/help/b7931dd8-3152-4d3a-a9b5-84621660c5f5.mspx?mfr=true. • For information about Windows® Mobile 5.0 to help protect mobile devices such as Pocket PCs, see http://www.microsoft.com/windowsmobile/business/5/default.mspx. Microsoft also supports multi-factor authentication, including the use of smart cards. For more information regarding the use of smart cards, see www.microsoft.com/technet/security/topics/networksecurity/securesmartcards/default.mspx.
MR079	Departments that need to destroy or dispose of IT media containing classified or protected information must follow the methods and procedures defined in associated technical documentation.	Windows® Rights Management Services (RMS) can be used to establish expiration dates on documents which might be used to assist in the life cycle management of GoC information. For more information about RMS, see http://www.microsoft.com/rms.
Paragraph 16.2 – Storage, Disposal and Destruction of IT Media		
MR080	Departments must mark IT media containing classified or protected information in accordance with the Operational Security Standard on the Identification of Assets, and must, in accordance with the Operational	Microsoft provides technologies that can support policy-based labels, including labels associated with classified and protected information. Windows® Rights Management Services (RMS) technologies allow you to both label and protect the data in your organization based on organizational security policy. RMS applies encryption-based, policy-driven protection that travels with the information wherever it goes. For more information about RMS, see http://www.microsoft.com/rms.

	Security Standard on Physical Security.	
Paragraph 16.3 – Personnel Security in the IT Security Environment		
MR081	The security requirements for personnel screening in section 10.9 of the GSP and the Operational Security Standard on Security Screening apply to positions and contracts requiring access to information and assets relating to information technology and ITS. In addition, departments must screen, to at least the secret level, all personnel with privileged access to critical systems.	
Paragraph 16.4.1 – Selection of Security Products		
MR082	Departments should consider the cost, quality, effectiveness, ease-of-use, assurance, and impact on the performance of the department's systems when selecting security products.	Information is provided throughout this matrix that would assist GoC departments in the evaluation of Microsoft products. Some of the more relevant items to consider include: • Microsoft's critical and internet-facing software must undergo a rigorous Security Development Lifecycle (SDL) process before it is approved for release. See MR074 for additional information. • A number of Microsoft's products have been successfully evaluated against the Common Criteria. See MR074 for additional information. • Microsoft's product offerings are in-line with the GoC's defence-in-depth strategy, and we are offering more comprehensive security solutions in response to an ever-increasing threat environment.
MR083	Departments should use evaluated products, especially in systems where the security afforded by that product is assured. Evaluated products should be evaluated based on ISO/IEC 15408, the Common Criteria for Information Technology	See MR042.

	Security Evaluation.	
Paragraph 16.4.2 – Identification and Authentication		
MR084	Departments must incorporate identification and authentication safeguards in all their networks and systems, according to the level or risk for the network or system.	Microsoft provides the following general guidance on identity management solutions: • For fundamental information about identity management, see http://www.microsoft.com/technet/security/topics/identitymanagement/idmanage/P1Fund_0.mspx. • For information about identity management platform and infrastructure, see the "Platform and Infrastructure" paper at http://www.microsoft.com/technet/security/topics/identitymanagement/idmanage/P1Plat_0.mspx. • For information about the security of services and service accounts, see The Services and Service Accounts Security Planning Guide at http://www.microsoft.com/technet/security/topics/serversecurity/serviceaccount/default.mspx. • For information about intranet access management, see http://www.microsoft.com/technet/security/topics/identitymanagement/idmanage/P3Intran_0.mspx. • For information about extranet access management, see http://www.microsoft.com/technet/security/topics/identitymanagement/idmanage/P3Extran_0.mspx. • For information about identity aggregation and synchronization, see http://www.microsoft.com/technet/security/topics/identitymanagement/idmanage/P2Ident_0.mspx. Microsoft also provides the following specific examples on identity management solutions: • For information about directory services administration, see Service Management Functions: Directory Services Administration at http://www.microsoft.com/technet/itsolutions/cits/mo/smf/smfdirsa.mspx. • For information about Active Directory, see http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx. • For information about how to secure Active Directory administrative groups and accounts, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/activedirectory/sec_ad_admin_groups.mspx. • For information about Active Directory Federation Services (ADFS), see http://www.microsoft.com/WindowsServer2003/R2/Identity_Management/ADFSwhitepaper.mspx. • For information about deploying and operating a PKI, see http://www.microsoft.com/technet/itsolutions/msit/security/deppkiin.mspx. • For information about how to build an enterprise root CA in small and medium businesses, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/windowsserver2003/build_ent_root_ca.mspx. • For information about Microsoft's Certificate Lifecycle Manager

		(CLM), see http://www.microsoft.com/windowsserversystem/CLM/overview.mspx.
MR085	When assigning a unique identifier for users, departments must ensure the proper identification of the individual to whom the identifier is issued.	
Paragraph 16.4.3 – Authorization and Access Control		
MR086	Departments must restrict IT and information access to individuals who have been screened and authorized; have been identified and authenticated; and have a "need to know."	Much of the directory service within the Microsoft® Windows® 2000 Server and Windows Server® 2003 operating systems focuses on authentication, authorization, and access control. Internet Authentication Service (IAS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy. As a RADIUS server, IAS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless and virtual private network (VPN) connections. As a RADIUS proxy, IAS forwards authentication and accounting messages to other RADIUS servers. Microsoft provides the following general guidance on these access control solutions: • For information about securing administrator accounts, see The Administrator Accounts Security Planning Guide at www.microsoft.com/technet/security/topics/serversecurity/administratoraccounts/default.mspx • For information about how to select secure passwords, see Selecting Secure Passwords at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/select_sec_passwords.mspx. • For information about how to enforce strong password usage, see Enforcing Strong Password Usage Throughout Your Organization at www.microsoft.com/technet/security/smallbusiness/topics/networksecurity/enforce_strong_passwords.mspx. • For information about deploying and operating public key infrastructure (PKI), see Deploying PKI Inside Microsoft at www.microsoft.com/technet/itsolutions/msit/security/deppkiin.mspx • For information about how to build an enterprise root certification authority in small and medium businesses, see Building an Enterprise Root Certification Authority in Small and Medium Businesses at www.microsoft.com/technet/security/smallbusiness/prodtech/windowsserver2003/build_ent_root_ca.mspx. Microsoft provides the following specific examples on these access control solutions: • For information about using IAS, see Internet Authentication Service at www.microsoft.com/windowsserver2003/technologies/ias/default.mspx. • For information about how to use smart cards to secure access,

		see The Secure Access Using Smart Cards Planning Guide at www.microsoft.com/technet/security/topics/networksecurity/securesmartcards/default.mspx. • For information about using certificate services to secure wireless local area networks, see Securing Wireless LANs with Certificate Services at http://go.microsoft.com/fwlink/?linkid=14843. • For information about using Protected Extensible Authentication Protocol (PEAP) and passwords to secure wireless LANs, see Securing Wireless LANs with PEAP and Passwords at http://go.microsoft.com/fwlink/?linkid=23459. In addition, Role-Based Access Control (RBAC) is supported with Windows Server® 2003 Authorization Manager (AzMan). For additional information, see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetserv/html/AzManRoles.asp?_r=1. Microsoft also provides technologies that can support policy-based labels and enforce access restrictions to information as it flows from one department to another. Windows® Rights Management Services (RMS) technologies allow you to both label and protect your data based on organizational security policy. RMS applies encryption-based, policy-driven protection that travels with the information wherever it goes. For more information about RMS, see http://www.microsoft.com/rms. Furthermore, User Account Protection will be supported in Windows Vista™, the next major release of the Windows® OS. This will isolate administration functions from general user functions. For additional information about Windows Vista security features, see http://www.microsoft.com/technet/windowsvista/evaluate/feat/secfeat.mspx. Additional information with respect to identity management is provided under MR084. For a generic paper on access control, see: http://download.microsoft.com/download/d/3/f/d3f4fe20-b522-40b8-8975-eb6f3076bdfd/Access_Control_WP.doc.
MR087	Departments must keep access to the minimum required for individuals to perform their duties (i.e., the least-privilege principle), and ensure that they are regularly updated to accurately reflect the current responsibilities of the individual.	See MR086.

MR088	Departments must withdraw access privileges from individuals (including students, contractors, or others with short-term access) who leave the organization, and revise access privileges when individuals move to jobs that don't require the same level of access	See MR086.
Paragraph 16.4.4 – Cryptography		
MR089	Departments must ensure effective key management, including the protection and recovery of cryptographic keys.	Microsoft's key management solutions include the protection and recovery of cryptographic keys. Refer to specific product guidance for additional information. (Pointers to specific product examples will be included in the next release of this guide.)
MR090	Departments must use encryption or other safeguards endorsed or approved by the Communications Security Establishment (CSE) to protect the electronic communication of classified and Protected C information	Microsoft provides several solutions for data classification and data protection. Windows® Rights Management Services (RMS) technologies allow you to both classify and protect the data in accordance with your organization's security policy. RMS applies encryption-based, policy-driven protection that travels with the information wherever it goes. Additional data protection technology solution examples include Internet Protocol security (IPsec) and Encrypting File System (EFS). IPsec provides data integrity and encryption to IP traffic, whereas EFS encrypts files stored in the file systems of Microsoft® 2000, Windows® XP Professional, and Windows Server® 2003. Microsoft provides the following guidance on these data classification and protection solutions. • For more information about RMS, see http://www.microsoft.com/rms. • For more information about the information rights management capabilities of Office 2003, see http://www.microsoft.com/technet/prodtechnol/office/office2003/operate/of03irm.mspx. • For more information about Windows® Rights Management Services partner offerings, see http://www.microsoft.com/windowsserver2003/partners/rmspartners.mspx. • For information about IPsec, see http://www.microsoft.com/windowsserver2003/technologies/networking/ipsec/default.mspx. • For information about how to use IPsec and Group Policy to isolate servers and domains, see http://go.microsoft.com/fwlink/?linkid=33945. • For more information about EFS, see http://go.microsoft.com/fwlink/?linkid=46681.

		• For information about how to use EFS to protect data, see http://www.microsoft.com/technet/security/smallbusiness/topics/cryptographyetc/protect_data_efs.mspx. • For information about how to protect sensitive information from theft, see http://www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/efsxppro.mspx. In addition, full volume encryption will be supported in Vista Enterprise Edition. The encryption algorithm used is AES-128 or AES-256. AES is endorsed by CSE. Microsoft will also offer pluggable crypto via the Crypto Next Generation (CNG) API and we will also support Suite B cryptography (also endorsed by CSE). The Vista Enterprise Edition will be available by the end of CY2006. For additional information regarding the security features that will be available with Vista, see http://www.microsoft.com/technet/windowsvista/evaluate/feat/secfeat.mspx.
MR091	Departments must encrypt protected B information before transmitting it across the Internet or a wireless network	See MR090.
Paragraph 16.4.5 – Public Key Infrastructure		
MR092	Public Key Infrastructure (PKI) is one way that departments can fulfill requirements for authentication, confidentiality, integrity and non-repudiation. Note: While this may not be considered to be a mandatory requirement, many GoC departments utilize PKI and therefore this requirement was included.	Microsoft offers PKI products, including PKI for Windows® 2003. For additional information see http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx. For information about how Microsoft deployed and operates our own internal PKI, see http://www.microsoft.com/technet/itsolutions/msit/security/deppkiin.mspx.
Paragraph 16.4.6 – Network Security and Perimeter Defence		
MR093	Departments must segregate networks into IT security zones and implement perimeter defence and network security safeguards.	Microsoft has numerous sources of information and products related to network security. For example, Microsoft has published a guide that provides an overview of security-related issues for networks, and describes how to plan a security monitoring system on Microsoft® Windows®–based networks. For more information, see http://www.microsoft.com/technet/security/topics/auditingandmonitoring/securitymonitoring/default.mspx. Microsoft has also developed the following general guidance and product information on network security: • For information about how to secure your network, see

		www.microsoft.com/technet/security/topics/networksecurity/secmod88.mspx. • For information about best practices for security, see www.microsoft.com/technet/security/bestprac/overview.mspx. • For information about how to secure the network perimeter in small and medium businesses, see www.microsoft.com/technet/security/smallbusiness/topics/networksecurity/sec_net_smb_per_dev.mspx. • For information about how to protect against network attacks, see www.microsoft.com/technet/security/smallbusiness/topics/networksecurity/prot_clients_net_attacks.mspx. • For information about how to protect access to network assets using Network Access Protection (NAP), see www.microsoft.com/windowsserver2003/technologies/networking/nap/default.mspx. • For information about virtual private networks for Windows Server 2003, see www.microsoft.com/windowsserver2003/technologies/networking/vpn/default.mspx. • For information about the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy, see www.microsoft.com/windowsserver2003/technologies/ias/default.mspx. • For information on the Internet Security and Acceleration (ISA) server, see http://www.microsoft.com/isaserver/default.mspx. • Microsoft® Systems Management Server (SMS) provides many methods to control network security, including such capabilities as update and hotfix management, version management, network device discovery, and monitoring. For more information about SMS, see www.microsoft.com/smserver/default.mspx. In addition, Microsoft has developed the following guidance on network design: • Internet Protocol Security (IPsec) is a framework of open standards to ensure private, secure communications over IP networks that uses cryptographic security services. For more information, see www.microsoft.com/windowsserver2003/technologies/networking/ipsec/default.mspx. • For information about how to use IPsec and directory service Group Policy to isolate servers and domains, see http://go.microsoft.com/fwlink/?linkid=33945. • For information about how to use quarantine services with virtual private networks, see the www.microsoft.com/technet/security/prodtech/windowsserver2003/quarantineservices/default.mspx. • For information about which server products and their subcomponents in the Microsoft® Windows Server System™ use network ports and protocols, see http://go.microsoft.com/fwlink/?linkid=34291. • For information about how to select routers and switches, see www.microsoft.com/technet/security/topics/networksecurity/secmod40.mspx. • For information about how to secure remote access to network

		resources, see www.microsoft.com/technet/security/smallbusiness/topics/networksecurity/sec_remote_access.mspx. • For information about how to use the Protected Extensible Authentication Protocol (PEAP) to secure your wireless network, see http://go.microsoft.com/fwlink/?linkid=23459.
MR094	Departments must strictly control all Public Zone interfaces, including all external uncontrolled networks such as the Internet, at a defined security perimeter.	In addition to the information provided under MR093, Microsoft has developed the following guidance on protecting the network perimeter: • For information about how to design a suitable firewall for your organization's perimeter network, see www.microsoft.com/technet/security/topics/networksecurity/secmod156.mspx. • For information about how to design a suitable firewall for your organization's internal network, see www.microsoft.com/technet/security/topics/networksecurity/secmod155.mspx. • For information about configuring the Windows Firewall feature of Microsoft® Windows® XP with Service Pack 2 (SP2) for individual computers, see www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/cfgfwall.mspx. • For information about how to use Group Policy to configure Windows® Firewall, see www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/fwgrppol.mspx. • For information about how Microsoft® Internet Security and Acceleration (ISA) Server 2004 can help provide network perimeter security, see www.microsoft.com/isaserver/default.mspx. • For a case study about using ISA Server 2004 in a hospital environment, see www.microsoft.com/resources/casestudies/CaseStudy.asp?CaseStudyID=15478. • For information about using ISA Server 2004 to meet HIPAA Guidelines, see www.microsoft.com/resources/casestudies/CaseStudy.asp?CaseStudyID=15402. • For a case study about using ISA Server 2000 to protect healthcare information in a hospital setting, see www.microsoft.com/resources/casestudies/CaseStudy.asp?CaseStudyID=13433.
MR095	Departments must use perimeter defence safeguards (e.g. firewalls, routers) to mediate all traffic and to protect servers that are accessible from the Internet.	In addition to the information provided under MR093, Microsoft has developed the following guidance on protecting the network perimeter: • For information about how to design a suitable firewall for your organization's perimeter network, see www.microsoft.com/technet/security/topics/networksecurity/secmod156.mspx. • For information about how to design a suitable firewall for your organization's internal network, see www.microsoft.com/technet/security/topics/networksecurity/secmod155.mspx. • For information about configuring the Windows® Firewall feature

		of Microsoft® Windows® XP with Service Pack 2 (SP2) for individual computers, see www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/cfgfwall.mspx. • For information about how to use Group Policy to configure Windows Firewall, see www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/fwgrppol.mspx. • For information about how Microsoft® Internet Security and Acceleration (ISA) Server 2004 can help provide network perimeter security, see www.microsoft.com/isaserver/default.mspx. • For a case study about using ISA Server 2004 in a hospital environment, see www.microsoft.com/resources/casestudies/CaseStudy.asp?CaseStudyID=15478. • For information about using ISA Server 2004 to meet HIPAA Guidelines, see www.microsoft.com/resources/casestudies/CaseStudy.asp?CaseStudyID=15402. • For a case study about using ISA Server 2000 to protect healthcare information in a hospital setting, see www.microsoft.com/resources/casestudies/CaseStudy.asp?CaseStudyID=13433.
Paragraph 16.4.7 – Mobile Computing and Tele-working		
MR096	Departments that allow personnel to access departmental information and IT assets, networks and systems from outside their government offices must establish procedures for such use.	Microsoft offers a number of products that can assist in remote access protection, including: • For information about Microsoft's Internet Authentication Service (IAS), see www.microsoft.com/windowsserver2003/technologies/ias/default.mspx. • For information about how to protect access to network assets using Network Access Protection (NAP), see www.microsoft.com/windowsserver2003/technologies/networking/nap/default.mspx. • For information about using Network Access Quarantine with Windows Server™ 2003, see http://www.microsoft.com/technet/itsolutions/network/vpn/quarantine.mspx. • For information about how to secure remote client and portable computers, see www.microsoft.com/technet/security/smallbusiness/topics/networksecurity/sec_remote_port_comp.mspx. • For information about Windows® Mobile 5.0 to help protect mobile devices such as Pocket PCs, see http://www.microsoft.com/windowsmobile/business/5/default.mspx. • For information about Outlook® Web Access features in Exchange Server 2003, see http://www.microsoft.com/exchange/evaluation/features/OWA_Features.mspx.
MR097	Departments must ensure that	Education and awareness training for users is an essential ingredient to the success of any comprehensive security solution. Microsoft

	personnel working off-site are made aware of their security responsibilities, including the sensitivity and criticality of the information and IT assets they access.	assists in security awareness through the Security Cooperation Program (SCP) as well as providing on-line education and training material. Security-related information can be found on-line at: http://www.microsoft.com/security/. Additional product specific information is provided throughout this matrix.
Paragraph 16.4.8 – Wireless Devices		
MR098	Departments must apply appropriate safeguards and restrict the use of such devices to individuals who have received departmental approval.	For information about Windows® Mobile 5.0 to help protect mobile devices such as Pocket PCs, see http://www.microsoft.com/windowsmobile/business/5/default.mspx.
MR099	Users must turn off wireless devices with a voice transmission capability when attending a meeting at which sensitive information, above Protected A, is being shared.	Education and awareness training for users is an essential ingredient to the success of any comprehensive security solution. Microsoft assists in security awareness through the SCP as well as providing on-line education and training material. Security-related information can be found on-line at: http://www.microsoft.com/security/. Additional product specific information is provided throughout this matrix.
Paragraph 16.4.10 – Telecommunications Cabling		
MR100	Departments need to protect telecommunication cabling from unauthorized interception and damage. Departments must authorize, control and monitor access to telecommunication wiring, spaces and pathways (i.e., telecommunication rooms, main terminal rooms and other equipment rooms) in a manner appropriate for the sensitivity level of the information being transmitted.	

Paragraph 16.4.11 – Software Integrity and Security Configuration		
MR101	Departments must configure their systems to control the use of mobile code (e.g. Javascript).	Microsoft provides guidance on systems hardening guidance and security best practices. See MR006 for additional information.
MR102	Departments must implement safeguards to "harden" software that is exposed to the Internet (e.g. Web servers and their software) or servers supporting sensitive applications.	See MR006.
Paragraph 16.4.12 – Malicious Code		
MR103	Departments must install, use and regularly update antivirus software and conduct malicious code scans on all electronic files from external systems.	Microsoft provides a number of tools and products that address malicious code, including: • For information regarding the Malicious Software Removal Tool (MSRT), see http://www.microsoft.com/malwareremove. • For information about antispyware solutions, see www.microsoft.com/athome/security/spyware/software/default.mspx. • For information about Microsoft efforts to address spyware, see http://go.microsoft.com/fwlink/?linkid=47178. • For information about how to protect servers from viruses, worms, and spam, see www.microsoft.com/windowsserversystem/solutions/security/sybari.mspx. • For information about a holistic approach to virus protection, see The Antivirus Defense-in-Depth Guide at www.microsoft.com/technet/security/topics/serversecurity/avdind_0.mspx. • For recent security alerts and information, see http://www.microsoft.com/security/incident/default.mspx. • For information related to Microsoft® Client Protection to be available in 2006, see http://www.microsoft.com/windowsserversystem/solutions/security/clientprotection/default.mspx.
MR104	Departments must install new virus definitions as soon as practical.	Microsoft provides anti-virus and other anti-malware signatures on a regular basis. Enterprises will be able to download signature updates using standard update software. Microsoft provides tools to help enterprise customers manage software updates and patches, including: • For information about how to use Systems Management Server 2003 for patch management, see http://www.microsoft.com/technet/itsolutions/cits/mo/swdist/pmsms/2003/pmsms031.mspx.

		• For information about Windows® Server Update Services (WSUS) for Windows Server® 2003, see www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/wsus/default.mspx.
Paragraph 17 – Detection		
MR105	To protect information and ensure service delivery departments must continuously monitor system performance to rapidly detect: - attempts (failed or successful) to gain unauthorized access to a system, or to bypass security mechanisms - unauthorized probes or scans to identify system vulnerabilities - unplanned disruption of systems or services - denial-of-service attacks - unauthorized changes to system hardware, firmware, or software - system performance anomalies, and - known attack signatures.	Microsoft offers several products that can help continuously monitor systems, including: • Microsoft® Baseline Security Analyzer (MBSA) tool see http://www.microsoft.com/technet/security/tools/mbsahome.mspx, • Microsoft® Operations Manager (MOM) – see http://www.microsoft.com/mom/evaluation/default.mspx • Systems Server Manager (SMS) – see http://www.microsoft.com/smserver/evaluation/default.mspx • Microsoft® Office Business Scorecard Manager - see http://office.microsoft.com/en-us/FX012225041033.aspx. In addition, the next version of MOM (named System Center Operations Manager 2007) will include a security event audit feature for capturing and reporting on security events. To obtain additional information, see http://www.microsoft.com/mom/evaluation/beta/opsmgroverview.mspx. Microsoft also has produced a security monitoring and attack detection guide for security professionals that provides information on the detection and monitoring process. For more information about this resource, see www.microsoft.com/technet/security/topics/auditingandmonitoring/securitymonitoring/default.mspx. The Microsoft Management Server group has worked with partners to develop IT security and regularity compliance solutions. Two of these partners have developed specific add-on packs that audit key compliance controls for IT resources to support compliance governance efforts. The add-on packs provide event collection, alert templates, and reporting services to track monitoring and reporting requirements for regulations, such as SOX, GLBA, and HIPAA. For more information on MOM partners and the add-on packs, see www.microsoft.com/management/mma/catalog.aspx. For specific monitoring and reporting solutions relative to Microsoft® Rights Management Services (RMS), see http://www.microsoft.com/rms. For specific monitoring and reporting solutions relative to SQL: • For more information about the Microsoft® Office Excel® add-in for SQL Server Analysis Services, see http://www.microsoft.com/office/solutions/accelerators/exceladdin/default.mspx. • For more information about Microsoft® SQL Server 2000 Reporting Services, see www.microsoft.com/sql/reporting/default.mspx. • For information about the security features of SQL Server 2000 SP3, see www.microsoft.com/technet/prodtechnol/sql/2000/maintain/sp3sec

		00.mspx. For additional dashboard type reporting solutions, see the following resources: • For information about dashboard and reporting services from Microsoft partners, see www.microsoft.com/sql/reporting/partners/component.asp. • For more information about building financial reporting dashboards see http://www.microsoft.com/office/showcase/findashboard/default.mspx. • For information about business intelligence for reporting services from Microsoft partners, see www.microsoft.com/sql/reporting/partners/bi.asp.
MR106	At a minimum, departments must include a security audit log function in all IT systems. Departments must incorporate automated, real-time, incident detection tools in high risk systems.	See MR105.
Paragraph 18 – Response and Recovery		
MR107	Departments (must) establish mechanisms to respond effectively to IT incidents and exchange incident-related information with designated lead departments in a timely fashion.	See MR009.
MR108	Departments must appoint an individual or establish a centre to coordinate incident response and act as a point of contact for communication with respect to government-wide incident response.	See MR009.
Paragraph 18.3 – Incident Response		
MR109	Departments must develop incident response procedures to	See MR009.

	follow in order to mitigate damage, contain the cause of the incidents and restore services.	
MR110	Departments must always, when responding to an IT security incident, consider the impact of their actions or inaction on other federal organizations.	See MR009.
MR111	Departments must maintain operational records that show how incidents were handled, documenting the chain of events during the incident, noting the time when the incident was detected; the actions taken; the rationale for decisions; details of communications; management approvals or direction; and external and internal reports.	See MR009.
Paragraph 18.4 – Incident Reporting		
MR112	Departments must: • report incidents and threats to, and share information, subject to applicable legislation and relevant policies, about the incidents and the effectiveness of their response with PSEPC • participate in threat and risk briefings and teleconferences • provide PSEPC	See MR009.

	with current 24/7 contact information for the IT Security Coordinator or designate as well as a secondary point of contact • establish a procedure for notifying the appropriate operational personnel, managers and all affected parties, keeping contact lists up to date. (e.g., The IT Security Coordinator, the Departmental Security Officer, the Chief Information Officer, business or system managers) • notify the appropriate law enforcement agency if the incident appears to be criminal and the Canadian Security Intelligence Service if the incident has national security implications.	
Paragraph 18.5 – Recovery		
MR113	Before reconnecting or restoring services, departments must ensure that all malicious software has been removed and that there is no potential for recurrence or spread.	See MR019.
MR114	Departments must restore essential	See MR019.

	capabilities within the time constraints and the availability requirements specified in the departmental Business Continuity Plan.	
MR115	Departments must back up data regularly.	See MR019.
MR116	Departments must test backups regularly to ensure that they can be used for recovery.	See MR019.
MR117	Departments must back up all software and configuration data.	See MR019.
MR118	Departments must facilitate the restoration of data and services by allowing systems to undo operations and return to an earlier state (e.g., rollback services).	See MR019.
MR119	Departments must test restoration procedures regularly to ensure that they are effective and that they can be completed within the time allotted for recovery.	See MR019.
MR120	Departments must determine retention periods for essential business information and archived backups	See MR019.
MR121	Departments must document, in a memorandum of understanding or other agreement, all arrangements for off-site backup (in case the off-site backup is with	See MR019.

	another party).	
Paragraph 18.6 – Post-Incident Analysis		
MR122	For every severe or major IT security incident that occurs, departments must perform a post-incident analysis which summarizes the impact of the incident, including cost, and identifies: - security deficiencies; - measures to prevent a similar incident; - measures to reduce the impact of a recurrence, and - improvements to incident-handling procedures.	See MR009.
MR123	When requested by PSEPC, departments must share the lessons they learn from their post-incident analysis.	See MR009.