Microsoft Solutions for Security and Compliance

Regulatory Compliance Planning Guide

Microsoft

Contents

Introduction

The *Regulatory Compliance Planning Guide* is designed to help IT managers and Microsoft customers meet specific IT compliance obligations that directly relate to major regulations and standards. The guide introduces a framework-based approach that you can use as part of your efforts to comply with these regulations and standards. The guide also describes Microsoft products and technology solutions that you can use to implement a series of IT controls to help meet your regulatory obligations.

This guide is not a comprehensive resource on regulatory compliance for every organization. For answers to specific regulatory compliance questions that concern your organization, consult your legal counsel or auditor.

The introduction for this guide includes the following sections:

- **Executive Summary**. This section provides a broad overview of the regulatory environment and the primary goals of the planning guide. It discusses what knowledge IT managers need so that they can then start to address their regulatory compliance requirements.
- **Who Should Read This Guide**. This section describes the audience for this guide, its purpose and scope, and caveats and disclaimers about the limitations of this guidance.
- **Regulations and Standards**. This section provides an overview of the five major regulations and standards that this guide discusses:
    - Sarbanes-Oxley Act (SOX)
    - Gramm-Leach-Bliley Act (GLBA)
    - Health Insurance Portability and Accountability Act (HIPAA)
    - European Union Data Protection Directive (EUDPD)
    - ISO 17799:2005 Code of Practice for Information Security Management (ISO 17799)
- **IT Controls**. This section discusses the various types of IT controls, how these controls work in combination, and why they are important components that your organization can use to help meet its regulatory compliance obligations.
- **IT Audit Process**. This section provides an overview of the IT audit process that auditors use to assess regulatory compliance for most organizations.
- **Business Drivers**. This section discusses the business drivers for regulatory compliance that include challenges concerning regulatory environment complexity, achieving and maintaining compliance, and the consequences of noncompliance. It also discusses opportunities to establish and improve process, gain competitive advantage, and increase ROI for your organization through time and cost savings.

Executive Summary

Regulatory compliance is a topic that few organizations can ignore. An ever-increasing number of regulations affect companies both large and small. The regulations and standards come from many sources, such as national and local governments. Examples include the Sarbanes-Oxley Act (SOX) and the California Law on Notice of Security Breach, formerly known as SB-1386. They also come from industry-specific oversight groups, such as the Payment Card Industry Data Security Standards.

What makes this situation even more complex is that any organization might need to comply with multiple sets of regulations, each of which mandates a separate set of requirements. Not surprisingly, many companies find it difficult to understand how to respond appropriately to these regulatory requirements, and then maintain their regulatory compliance through cost-effective processes and procedures. Finally, regulations often mention IT controls only in passing, and leave IT managers to determine exactly what they must do to achieve and maintain regulatory compliance.

The *Regulatory Compliance Planning Guide* is for IT managers who are responsible to meet the regulatory compliance obligations of their companies. The intent of this guide is to assist them in achieving two primary goals:

- First, to help IT managers better understand *what* they need to know to address their regulatory compliance requirements. To achieve this, the guide describes how IT managers can use a framework-based approach to compliance, and includes mappings of five common regulations and standards with which many organizations must comply.
- Second, to help IT managers understand *how* they can begin to address many of the IT control requirements that apply to their organizations. To achieve this, the guide provides information about solutions that you can use to address the regulatory compliance requirements for your organization.

Important This planning guide does not provide legal advice. The guide only provides factual and technical information about regulatory compliance. Do not rely exclusively on this guide for advice about how to address your regulatory requirements. For specific questions, consult your legal counsel or auditor.

Note The term *regulatory compliance* is actually a bit of a misnomer, because various obligations can come from laws, regulations, rules, and many other legal instruments, such as court judgments, litigation, and even contracts. To promote readability, this guide uses the term *regulatory compliance* to address compliance with all kinds of legal obligations, and *regulations* to refer to any requirements imposed by a governing body.

Who Should Read This Document

The *Regulatory Compliance Planning Guide* is primarily for IT managers who are responsible to ensure that appropriate safeguards and controls maintain privacy, security, and reliability for their organizations according to the mandates of various regulatory requirements. 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 Financial Officers (CFOs)** who are concerned with the overall control environment of their organizations.

- **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.

Guide Purpose

The purpose of this guide is to help your organization identify and implement available software, tools, and technology solutions to begin to address regulatory compliance requirements. To achieve these objectives, the guide first provides information that you can use to map regulations and standards to a *control framework.* The guide then illustrates the mapping of regulatory compliance controls to possible technology solutions.

The guide provides several benefits for your organization. It shows how you can apply a control framework to both present and future regulations and standards, which helps to make the process of interpreting regulatory requirements easier and more efficient. The guide also presents solutions and suggests software products that can help you implement the IT controls that your organization needs.

Guide Scope

The *Regulatory Compliance Planning Guide* provides the following for your organization:

- A sample control framework that addresses various regulations and standards that pertain to the privacy and security of sensitive information.
- A technological map to Microsoft resources that you can use to address control framework components.

The guide is divided into the following sections:

- **Introduction**. This section introduces the guide, defines the audience for it, and provides a brief overview of the regulations and standards that it addresses. This section also discusses IT controls, the IT audit process, and the business drivers for regulatory compliance.
- **Framework-Based Regulatory Compliance**. This section discusses how frameworks address regulatory compliance objectives and the benefits that they provide. It also introduces a sample control framework.

- **Mapping Regulations to Technology Solutions**. This section addresses the scope of the regulations and standards that the guide considers, and identifies specific components that map to the sample control framework. This section also provides an example of how the control categories in the sample framework map to regulation elements, which in turn map to specific technology solution sets.
- **Technology Solutions for Regulatory Compliance**. This section provides detailed information about specific Microsoft resources that your organization can use to help it address each of the control categories in the sample control framework to help achieve regulatory compliance effectively and efficiently.

Caveats and Disclaimers

The intention of this guidance is to help you understand some common compliance obligations that organizations encounter with laws and regulations, and what the laws and regulations require them to do. 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.

Regulations and Standards

Increased government oversight in recent years has resulted in new regulations that affect organizations in a wide range of industries. The *Regulatory Compliance Planning Guide* focuses on five significant regulations and standards that affect many companies. These major regulations and standards include:

- *Sarbanes-Oxley Act (SOX)*
- *Gramm-Leach-Bliley Act (GLBA)*
- *Health Insurance Portability and Accountability Act (HIPAA)*
- *European Union Data Protection Directive (EUDPD)*, which has resulted in other national legislation such as the *Personal Data Act (523/1999) and Amendment (986/2000)* of Finland.
- *ISO 17799:2005 Code of Practice for Information Security Management (ISO 17799)*

Although this guide does not specifically address other regulations and standards, the analysis in the guide also might assist you in addressing other regulatory compliance scenarios that apply to your organization, such as data breach legislation. This section provides a brief overview of each major regulation and standard.

Sarbanes-Oxley Act (SOX)

SOX was enacted in the United States in response to various corporate scandals. From an IT and internal control perspective, the most prominent part of SOX is Section 404. This section of the act requires publicly traded companies to assess the effectiveness of their internal controls for financial reporting in annual reports they submit at the end of each fiscal year. Section 404 also requires publicly traded companies to engage independent auditors who must attest to, and report on, the validity of their assessments. The U.S. Securities and Exchange Commission is the regulatory agency responsible for enforcing SOX.

Gramm-Leach-Bliley Act (GLBA)

GLBA, also know as the Financial Services Modernization Act of 1999, protects the privacy and security of private financial information that financial institutions collect, hold, and process. The privacy component of this act requires financial institutions to provide customers with an annual notice of their privacy practices, and to give them the option to direct financial institutions not to share such information. The safeguards component of the regulation requires financial institutions to establish a comprehensive security program to protect the confidentiality and integrity of the private financial information in their records. A number of U.S. federal agencies, including the Office of Thrift Supervision (OTS) and the Office of the Comptroller of the Currency (OCC), enforce GLBA.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA includes among its components privacy and security rules. These rules focus on Protected Health Information (PHI) and Electronic PHI (ePHI) that result from efforts to streamline the health care system in the United States, and mandate the standardization of electronic transactions, code sets, and identifiers. The privacy and security rules for this act are detailed and prescriptive. Although the regulation focuses on companies in the U.S. health care industry, it can extend to other companies if they engage in certain activities, such as managing employee group health plans, or providing services to companies that this regulation directly affects. Sub-departments of the U.S. Health and Human Services department (HHS) enforce HIPAA regulations.

European Union Data Protection Directive (EUDPD)

EUDPD provides baseline requirements that all European Union (EU) member states must achieve through national regulations to standardize the protection of data privacy for citizens throughout the EU. The directive has a strong influence on international regulations because of the limitations it places on sharing personal information about EU citizens outside of the EU in areas deemed to have less than adequate data security standards. Examples of specific laws in countries and regions representing EU member states include:

- *Personal Data Act (523/1999) and Amendment (986/2000)* of Finland
- *Act on Processing of Personal Data (Act No. 429 of 31 May 2000)* of Denmark
- *Federal Act Concerning the Protection of Personal Data (Datenschutzgesetz 2000 - DSG 2000*) of Austria

EUDPD and the regulations enacted pursuant to it affect companies that do business in the EU or handle the data of EU citizens. Various regulatory agencies of EU member states enforce the various national privacy regulations based on EUDPD.

ISO 17799:2005 Code of Practice for Information Security Management

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.

IT Controls

A control can be defined as “a device or mechanism used to regulate or guide the operation of a machine, apparatus, or system.” Organizations use controls to regulate their business processes, which include production, distribution, finance, and so on. Controls help organizations to restrain and correct atypical behavior, and to reduce and prevent the spread of problems and errors.

Many regulations have the sole purpose of ensuring that organizations have proper controls in place. For instance, HIPAA requires that proper controls over information security and privacy are in place to protect patient records. And SOX demands that publicly traded companies in the United States use controls to ensure that their financial statements are accurate.

Organizations implement controls to:

- Reduce the risk of fraud.
- Protect company assets.
- Prevent disclosure of company secrets.
- Comply with regulations.
- Improve business awareness.
- Improve efficiency.

At the highest level, you can divide controls into business controls and IT controls. Although all controls are put in place to address risks to the business, business controls and IT controls differ in how they are implemented. Business controls regulate and guide the business processes of the organization. For example, the requirement for management approval of purchase orders is a business control to prevent unnecessary expense. Business controls exist for nearly every process in an organization, from hiring, to purchasing, to sales, to financial reporting.

IT controls regulate and guide the operation of IT in the organization, including all of the processes, and systems within it. These controls focus on processes that concern IT managers, including availability, change management, user provisioning, security, and so on. It is these controls that are the focus of this planning guide.

General Controls and Application Controls

There are two broad IT control categories: general controls and application controls.

General Controls

General controls apply to the entire IT infrastructure of the organization. Organizations must have reasonable general controls in place before they can rely on their application controls. For example, if you are not confident of the overall security for the database server that holds your company’s enterprise resource planning (ERP) system data, can you really trust the data in the ERP system, no matter how many data validation checks the ERP system does on the data that it stores? If a malicious attacker can bypass the

application controls because of a weakness in the general controls, the whole network for the organization is at risk.

General controls focus on many areas of responsibility for IT managers, including:

- IT organization
- Policy creation and communication
- System security
- Operations
- Change management
- Incident handling
- Monitoring
- Performance

Applications Controls

Application controls are unique to each application that your organization uses to run its business. In this respect, application controls are the IT components that enforce business controls. Application controls help to minimize mistakes and prevent or detect malicious actions, such as fraud. Because application controls are so closely tied to the business processes their applications support, these controls are often considered business controls implemented by information technology.

Application controls focus on:

- **Data preparation procedures**. Procedures for these controls help to minimize errors and omissions. For example, during data origination, error-handling procedures help to detect, report, and correct errors that are specific to the data.
- **Accuracy, completeness, and authorization checks**. Procedures for these controls help to ensure change control and validation for input data as close to its point of origin as possible. Transaction data processing is subject to a variety of procedural controls to enforce these checks.
- **Data processing integrity**. Procedures for these controls help to ensure separation of duties and work effort verification. Examples include update controls to verify totals and master file update controls.
- **Output distribution**. Procedures for these controls help to ensure consistency and management policy. Examples include controls that define, communicate, and adhere to management policies for IT output distribution.
- **Sensitive information transmission protection**. Procedures for these controls help to ensure that adequate protective measures are in place to prevent unauthorized access and tampering of sensitive information during transmission and transport.

The following figure illustrates the relationships of the various types of controls.

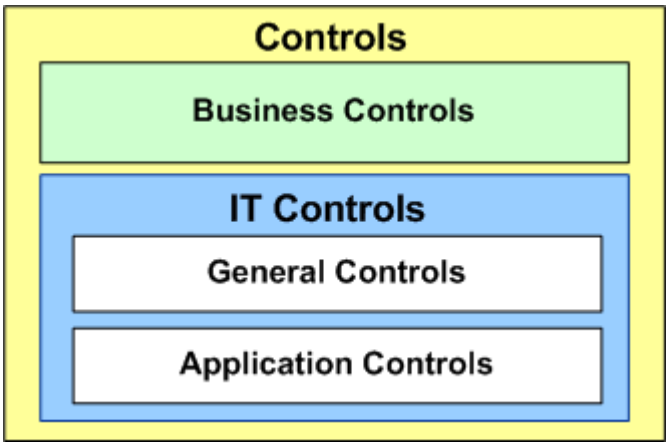

Figure 1. Broad types of controls

Further Classification of IT Controls

There are two other ways to further classify IT controls. First, controls can be classified as either *manual* or *automated*. Manual controls require a person to enforce the control, whereas the IT system enforces automated controls. Second, you can also classify IT controls as either *preventive* or *detective*. As the name indicates, preventive IT controls prevent unwanted events from occurring. Detective IT controls cannot prevent unwanted events, but they can detect events and then notify a person or system to respond to them.

Based on these factors, four types of IT controls are possible as the following figure illustrates.

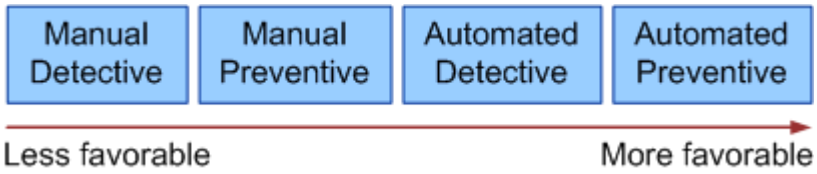

Figure 2. The four types of IT controls

A password complexity policy provides a good example of the various types of IT controls and how they work. Suppose an organization has a requirement—either from a regulation or as part of their security policy—that passwords must be no fewer than eight characters long. There are a number of ways to meet this requirement, depending on the type of controls that the organization implements. The following IT control examples provide different ways to meet this requirement:

- **Manual detective**. This type of control requires a person in the organization to determine manually if an unwanted event has taken place. For this example, the organization could institute a manual detective control that would require an administrator to run a report once a week to find any passwords fewer than eight characters long. When the results of the report detect an insufficient password, the administrator can take some action, such as to disable the account or send a note to the offending user's manager. Manual detective controls are generally inefficient because they require human effort both to detect the problem and resolve it. For this reason, you should consider using manual detective controls only as a last resort when other types of controls are not available.

- **Manual preventive**. Sometimes a manual preventive control is sufficient to meet the objective. A manual preventive control in this case could require the organization to publish a password policy that requires all employees to use complex passwords at least eight characters long before they can access the organization's network. The intent of the control is to prevent short passwords, but it requires human compliance to be effective.
- **Automated detective**. This type of control allows a system to detect automatically unwanted events and notify the appropriate personnel to remediate them. For this example, an automated detective control could take the form of an automated process that scans for insufficient passwords and then notifies an administrator when it detects one. As in the manual detective example, the administrator would take action when a password problem is found.
- **Automated preventive**. When possible, an automated control is preferable because it eliminates the human factor of possible noncompliance. For this example, the organization could use an operating system capability that will not allow users to establish short passwords. This control meets the password policy requirements and is much more difficult for personnel to ignore or circumvent.

Note that because automated controls eliminate human involvement, they are generally considered more effective than manual controls. In addition, it is generally preferable to prevent problems than to detect and respond to them. Therefore, automated preventive controls are generally preferred over the other three control types.

Cumulative Controls

Sometimes a single control is not sufficient to meet an organization’s needs. In this case, more than one control might be necessary to reach the level of control that is required. When several controls combine to meet a specific control objective, they become *cumulative controls*.

Organizations often use cumulative controls when they must rely on manual controls, or when the risk that the organization faces is large in scope. For example, if a policy or manual preventive control is the only way to enforce a password length requirement, it also would be advisable to implement a manual or automated detective control to monitor the level of compliance.

Cumulative controls could also be helpful when your organization must address a significant risk. For example, running critical business functions on an obsolete operating system is generally considered a large security risk. However, if your organization has no other choice, you can implement other controls to compensate for this risk. In this case, you might not allow the vulnerable system to connect to the corporate network. In addition, you could prevent the use of removable media with the system to reduce the risk of malicious software infection. Any one of these controls might not be enough to address this problem. However, they can be effective when you combine them.

Why IT Controls Are Important

IT controls are important because they provide an efficient means for your organization to combine its business-focused requirements and regulatory compliance objectives. IT managers can implement IT controls to establish reliable processes to measure and improve the organization's IT control environment. Effective IT controls also position your organization to better adjust to changing regulatory compliance requirements.

It is also important to note that IT auditors greatly prefer to assess automated IT controls because they can evaluate them more quickly and reliably to determine the quality of the compliance efforts that the organization has in place. This can reduce the time, expense,

and disruption of your IT audits. This is in addition to the fact that automated controls are generally less expensive in the long term than manual controls.

The next section focuses on how auditors accomplish the IT audit process.

IT Audit Process

Audits are a critical component of the regulatory compliance process. In general, it is the auditors who will determine whether your organization is in compliance with the regulations and standards that it must address. For example, in regard to Sarbanes-Oxley (SOX), external auditors will often determine the adequacy of the internal controls in your organization as part of the audit in relation to annual financial reporting. Understanding how the audit process works and how auditors operate is important because it informs IT managers how to establish an environment that is compliant and easy to audit. This topic focuses on how auditors conduct the IT audit process.

It is important to understand what auditors look for during a compliance audit. During the audit, the auditors look for evidence that indicates:

- The organization has designed effective controls to address their compliance requirements and that there are no design deficiencies.
- The organization consistently applies the controls they have designed and that there are no operational deficiencies.

If the auditors do not find evidence of an effective control program, or they find that the organization is not adhering to the control program, they note these deficiencies in their final audit report. This audit report is generally provided to the organization’s audit committee so that identified issues get the appropriate level of management exposure. Obviously, it is preferable that there be no deficiencies noted in this report.

The following process describes the general activities that auditors conduct during an audit. Your auditor might conduct the audit using a slightly different approach:

- Step 1: Plan the audit (auditor)
- Step 2: Hold audit kickoff meeting (auditor/organization)
- Step 3: Gather data and test IT controls (auditor/organization)
- Step 4: Remediate identified deficiencies (organization)
- Step 5: Test remediated controls (auditor/organization)
- Step 6: Analyze and report findings (auditor)
- Step 7: Respond to findings (organization)
- Step 8: Issue final report (auditor)

Understanding the steps in the IT audit process positions IT managers to know what to expect from the audit. In this way, you can better achieve your organization's regulatory compliance objectives, and optimize the audit process to complete it more efficiently.

Step 1: Plan the Audit

To plan for the audit, the auditor requires the organization to provide a list of all IT controls that it currently uses, in addition to documentation that defines how each control works. The documentation should describe how the controls minimize risk for the organization and address their compliance requirements. The auditor uses these documents to determine the design adequacy of the IT controls in your organization.

The audit team typically determines the scope of IT controls that the auditor focuses on in the organization. The scope depends on the type of audit being performed. In a SOX audit, for example, the scope of the audit will be the primary financial accounts and the mission-critical applications that support them. The auditors also use the planning phase to define any areas that might require special focus. They might base this on areas of weakness noted in a previous audit, guidance from regulatory agencies, or a risk assessment of the current environment. It is very useful to be aware of the scope of the audit to be as prepared as possible for it.

Step 2: Hold Audit Kickoff Meeting

The auditor and organization meet to kick off the IT audit process and confirm the audit plan for the organization. In addition, the auditor will use this opportunity to identify which of the organization's resources will be required to support the audit process.

Step 3: Gather Data and Test IT Controls

Next, the auditors conduct tests to ensure that the documented controls are in place and working appropriately. The number and type of tests that the auditors conduct depend on the type of controls that they test, in addition to the criticality of the system that the IT controls address.

For example, an IT administrator might demonstrate to the auditor how users complete and submit a form to create access for themselves to the system. The auditor verifies that the information requested of the user meets both regulatory and operational requirements. For manual controls related to this process, the auditor examines the validity and thoroughness of policy documentation for the organization in the same manner. The auditor will also verify that appropriate approvals are obtained.

Step 4: Remediate Identified Deficiencies

Based on the test results, the auditors inform the organization of any issues they have identified. In some cases, it will be possible for the organization to address these issues relatively quickly. When such deficiencies are identified, the auditors might allow some time for the organization to correct them.

Step 5: Test Remediated Controls

The auditors conduct tests on the remediated IT controls. The auditor can either accept or reject that the deficiencies have been adequately addressed. If the auditor finds that the organization has adequately addressed the deficiencies, the auditor might not include these deficiencies in the final audit report.

Step 6: Analyze and Report Findings

When all testing is complete, the auditors compile their findings in a report. This report will detail any deficiencies discovered during the audit. Deficiencies can fall into one of the following categories:

- **Design deficiencies**: These are situations in which the auditor finds a complete or partial lack of controls for a given risk, or finds that the controls are not sufficient to adequately accomplish their goal. An example of a design deficiency is if the organization handles confidential customer information, such as a name, address, and drivers license number, but has no controls to document how it protects this information.
- **Operational deficiencies**: These are situations in which the auditor finds that the organization does not apply the controls as designed. This could occur if the control was documented but never put into production, or if the control is in production, but the organization does not adhere to it. For instance, a control may state that a vice president or higher level executive must approve a user's access request for a particular sensitive resource before the user is granted access. This would constitute an operational deficiency if the auditors determine that access is routinely granted without such approval.

The auditor produces a *summary of control deficiencies* report for the organization that includes the extent and number of exceptions that the organization needs to address.

Step 7: Respond to Findings

The organization is generally given a chance to respond to the auditors' findings, either with their view of any circumstances that could mitigate the findings, or with plans to address the auditors' findings in the future. Most organizations try to address the identified IT control deficiencies before their next audit.

Step 8: Issue Final Report

As the last step in this process, the auditor issues a final report for the audit. This report is shared with IT management, in addition to the financial audit team (if there is one) for inclusion in the overall audit report. The audit report might also be shared with the board of directors or appropriate third parties such as regulatory agencies.

How to Optimize the Audit Process

There are many ways to make the audit process more efficient and less difficult. These include:

- Work with the auditor early in the process to understand the key areas on which they plan to focus during the audit. In some cases, you can reprioritize projects to ensure that you address what the auditors see as key risks in the environment, thus avoiding deficiencies in the audit.
- Implement automated IT controls whenever possible. These controls are superior to manual ones because auditors can more easily test and validate them. The best way to optimize the efficiency and lower the cost of the IT audit process for your organization is to:
    - Maintain clean and concise documentation of IT controls and keep it updated.
    - Organize your IT controls to work with the framework that your auditors use. This will help ensure that you and your auditors communicate clearly about the regulatory objectives.

- Take advantage of an IT controls framework as described in Section 2, "Framework-Based Regulatory Compliance," of this guide. This will help you to more effectively address a variety of regulations with a single set of controls.

A control framework can provide you with planning options to realize IT control efficiencies for your organization. A framework links business requirements to IT activities through a consistent model. You can use this model to identify the IT resources you need to define and meet your organization's IT control objectives.

Business Drivers

Many companies view regulatory compliance as a daunting task from which they receive little in return. This could be a short-sighted point of view. Although regulatory compliance presents significant challenges, it also offers corresponding opportunities. This section discusses business challenges and opportunities related to regulatory compliance.

Business Challenges

Regulatory compliance presents a number of challenges, which include managing a complex regulatory environment, addressing the difficulty of achieving and maintaining compliance, and understanding the consequences of noncompliance.

Regulatory Environment Complexity

The regulatory environment has become increasingly complex as the number and breadth of regulations has increased. This added complexity places greater responsibility on organizations and executives to manage regulatory demands, and to provide meaningful evidence of compliance. Specific requirements for each regulation also vary, along with the scope of activities that apply to each regulation. A thorough analysis of each regulation is required to determine the best course of action for each organization. Organizations must be diligent to understand how regulations apply to their business, and practical about implementing controls and business practices to demonstrate compliance.

Achieving and Maintaining Compliance

Many organizations have found it difficult to achieve and maintain compliance with the various regulations that apply to them. In particular, many organizations find that their compliance efforts are more complex, time-consuming, and costly than originally anticipated. These difficulties often stem from attempting to attain compliance with multiple regulations at a specific time—even as the regulations often apply to separate departments of the organization. After your organization completes its initial compliance efforts, the next challenge is to maintain compliance in a cost-effective manner. The responsibility to maintain this ongoing effort often remains dispersed. Unclear lines of responsibility can limit your organization's ability to view regulatory compliance holistically and can increase the risk of duplicating efforts.

Noncompliance Consequences

Many businesses are compelled to address regulatory compliance to avoid the legal consequences of not complying. These consequences can extend beyond financial, civil, or criminal penalties to affect the organization’s reputation in the market and its ability to access the resources it needs to succeed.

The consequences of noncompliance vary from one regulation to another, but they can include:

- Significant fines (both personal and organizational)
- Jail time for grievous offences
- Lawsuits from shareholders and other parties
- Limited access to capital markets
- Limited ability to do business in specific jurisdictions
- Increased regulatory oversight
- Loss of reputation
- Loss of customer and business partner trust

The threat of these potential consequences provides significant motivation to organizations and their executives to manage regulatory compliance effectively and proactively.

Business Opportunities

Regulatory compliance not only presents challenges to overcome, it also offers opportunities for your organization. Such business opportunities include the chance to improve processes, create competitive advantage, and further integrate IT into your business to improve ROI.

Process Improvement

Most regulations require that organizations have documented and repeatable business processes, and that those processes have appropriate controls in place to prevent mistakes or fraud. Automated processes generally have more effective controls than manual processes, and auditors can generally rely on automated processes more than manual ones. For these reasons, many organizations can use regulatory compliance to justify automating inefficient manual processes. Although the primary justification for automating processes is to improve IT controls and the ability to repeat them, an added benefit is that this process improves efficiency.

Identity management provides a good example of how better process improves efficiency. Many auditors have drawn attention to the lack of IT controls around the user life cycle management process that involves user account and profile creation, modification, and deletion. To address this deficiency, companies have implemented automated identity management tools. Although the purpose of such tools is primarily to automate the IT controls around critical business processes, implementing them also improves the efficiency of the user management process.

Competitive Advantage

In many industries, strong or early adherence to regulations can create a competitive advantage for a company. Organizations that provide services to other businesses can benefit from early and provable compliance with regulations. This is because other organizations are more likely to do business with companies in compliance that are in a position to help them meet their own regulatory compliance requirements. Examples of companies that stand to benefit from this competitive advantage include IT outsource firms, service bureaus, and health insurance administration firms.

Privacy is another significant concern for businesses and individuals today. Strong compliance with privacy regulations also provides a competitive advantage for organizations. Organizations can market their compliance with privacy regulations to build trust and market share with consumers, and allay the prevalent concern over privacy and identity theft among the public. In addition, because compliance with the

European Union Data Protection Directive (EUDPD) is a prerequisite to doing business in some European countries, compliance with this regulation can open up new markets for a company's products and services.

IT Integration and ROI

Regulatory compliance requirements can help IT managers further integrate themselves into their organizations. Although many regulations do not specifically require IT-based controls, it is often IT management that ends up implementing the IT controls that the regulations strongly suggest. This increases the need for IT and business management to work closely together to solve the difficult task of regulatory compliance.

As IT managers become more trusted partners with management, they can use this trust to influence management to develop other IT initiatives that can result in efficency gains and cost savings for the company. Such an initiative could be to focus more closely on how to develop, maintain, and back up secure applications for your organization.

Framework-Based Regulatory Compliance

This section of the *Regulatory Compliance Planning Guide* introduces a framework-based approach to addressing regulations. It includes some information about framework fundamentals, and describes the benefits that frameworks provide organizations to meet their IT control objectives.

The section then shows the process the team used to map relatively nonprescriptive regulations and standards to specific technologies by way of a sample control framework. This mapping can help you simultaneously address many regulatory requirements. The framework also allows you to avoid overlapping efforts to address the IT control objectives for your organization.

This section includes the following topics:

- **Framework Fundamentals**. This topic explains the fundamentals of a framework-based approach to regulatory compliance.
- **How Frameworks Benefit Organizations**. This topic explains the benefits that you can take advantage of through a framework-based approach to regulatory compliance.
- **A Framework for Your Organization**. This topic introduces a sample control framework and the resources that the project team used to develop it.

Framework Fundamentals

As regulations and standards that influence information technology continue to increase, many organizations face the challenge of how to focus their compliance efforts to meet the requirements of multiple rules and regulations. For example, a publicly traded U.S.–based financial services firm might need to comply with requirements from several regulations, including those from Gramm-Leach-Bliley (GLBA), Sarbanes-Oxley (SOX), and various U.S. Securities and Exchange Commission (SEC) regulations.

Currently, a company that must meet the requirements of multiple regulations might address them as follows:

1. Review each regulation.
2. Determine the IT control requirements specific to each regulation.
3. Implement the appropriate controls.
4. Conduct an audit to determine the compliance level.

Unfortunately, these steps are inefficient because the company has to repeat all of them to address each regulation. The following figure illustrates the inefficiency of this process.

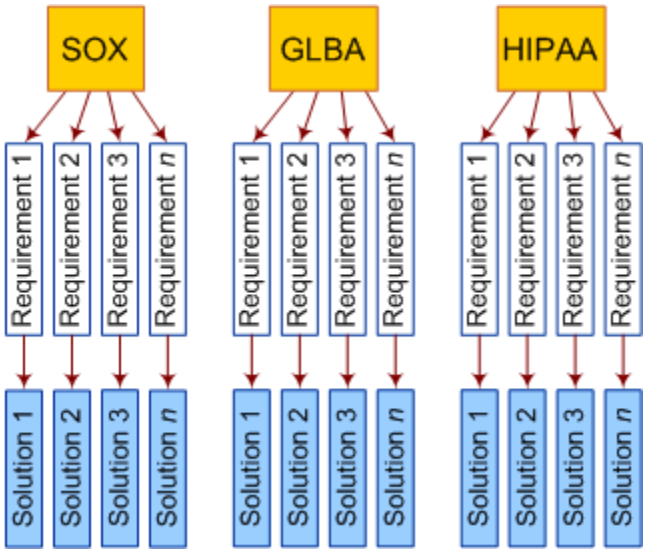

Figure 3. Addressing regulations inefficiently outside of a framework

Developing Common IT Controls

This guide recommends a different approach to regulatory compliance. Instead of viewing each regulation separately, it provides you with a means to consider all of the major regulations and standards that the guide includes at the same time to meet your organization's IT control objectives.

Many common regulations and standards that organizations must apply significantly overlap in the IT controls that they require. To make this process more efficient, often you can implement a single IT control to help address the compliance requirements for a number of regulations and standards.

For example, regulations such as HIPAA, GLBA, SOX, and laws based on the EUDPD, require management to establish procedures to ensure that actions to request, establish, issue, suspend, and close user accounts occur in a controlled manner. Establishing one set of IT controls to help address these user account life cycle requirements for all these regulations improves the efficiency and effectiveness of the organization’s compliance efforts.

The following figure illustrates how you can use IT controls simultaneously to help address many primary regulations and standards.

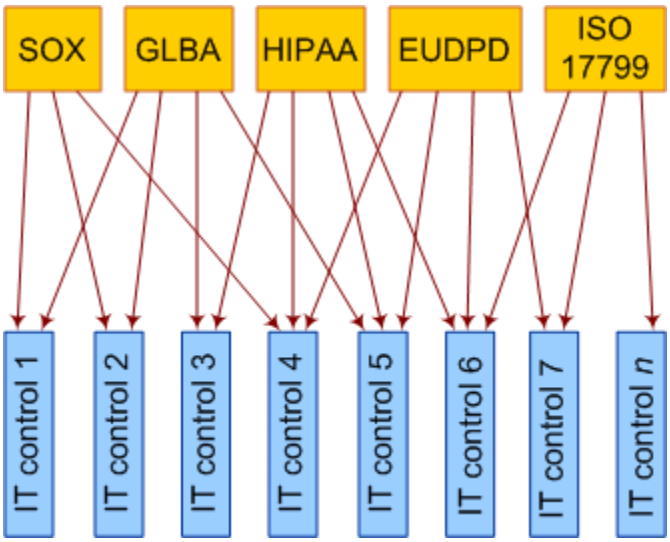

Figure 4. IT controls can address many regulations and standards simultaneously

The next topic, How Frameworks Benefit Organizations, describes how a well thought out regulatory compliance framework provides many benefits for your organization in addition to those mentioned in this topic.

How Frameworks Benefit Organizations

A framework provides many significant benefits for organizations seeking to achieve their regulatory compliance objectives. The framework-based approach to regulatory compliance allows organizations to:

- Combine IT controls to meet multiple regulatory standards, such as those from SOX and HIPAA, to avoid separate audits.
- Address new regulations rapidly as they are introduced.
- Prioritize spending on only those IT controls that will achieve the most impact.
- Avoid duplicating work to meet compliance objectives in different business units within the company.
- Update current regulations more efficiently through incremental changes to your organization's existing IT controls.
- Establish a common ground between the IT department and auditors.

The following figure illustrates how a control framework simplifies regulatory compliance for your organization.

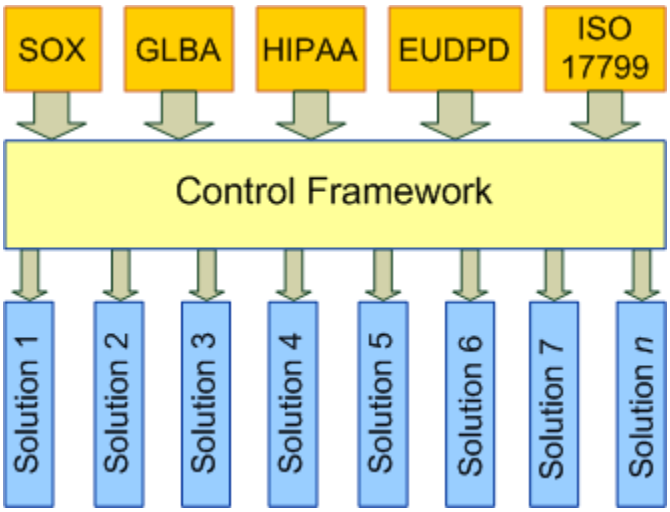

Figure 5. A conceptual view of a control framework

The final topic in this section describes how you can use a control framework to achieve all of these regulatory compliance benefits for your organization.

A Framework for Your Organization

Microsoft recommends that you use a control framework to help address your organization's regulatory compliance objectives effectively. Using a control framework enables your organization to map applicable regulations and standards to the framework. Then your organization can more efficiently focus its IT control efforts on addressing the requirements defined in the framework rather than individual regulations.

In addition, as new regulations and standards affect the organization, you can map them to the framework, and then concentrate your efforts on those parts of the framework in which the requirements have changed. Moreover, you can map a wide variety of IT control–related requirements to the framework, including industry-specific requirements, such as the Payment Card Industry security requirements, internal policies, and so on.

Microsoft recommends that organizations use an IT control framework to organize their regulatory compliance efforts. Several frameworks exist that could be used as a basis for this framework. These include the following control frameworks:

- IT Governance Institute (ITGI) Control Objectives for Information and related Technology 4th Edition (COBIT 4.0)
- ISO 17799:2005 Code of Practice for Information Security Management
- The British Office of Government Commerce IT Infrastructure Library (ITIL)
- The Microsoft Operations Framework (MOF)
- American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants (AICPA/CICA) Trust Services Framework
- American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants (AICPA/CICA) Privacy Framework

The next section, Mapping Regulations to Technology Solutions, focuses on using a control framework to map the regulations and standards to technology solutions.

Mapping Regulations to Technology Solutions

This section of the *Regulatory Compliance Planning Guide* focuses on mapping regulations to technology solutions. It introduces and defines the process that the team developed to translate relatively nonprescriptive regulations to specific technologies that can help address regulatory compliance and privacy assurance objectives.

This section uses two IT control maps to present this process. Each map provides a grid with technology solution categories. Each intersection in the maps indicates if the relevant technology solution category can address the regulatory and privacy requirements of that IT control. Finally, this section provides an applied example and a summary of this process.

This section includes the following topics:

- **Mapping Regulations to a Control Framework**. This topic presents an overview of how the major regulations and standards map to specific technology solution categories using a sample control framework.
- **Technology Solutions for Regulatory Compliance**. This topic presents the technology solution categories that are relevant to regulatory compliance.
- **Technology Solutions for IT Control**. This topic shows how each of the control framework categories maps to specific technology solutions. IT managers can use this map to determine the IT control types that they want to implement.
- **Applied Example**. This topic demonstrates how specific regulations drive specific technology solutions through an applied example. It is based on the earlier mappings in this section of the guide.
- **Summary**. This topic briefly reiterates the main points of this section of the guide.

Mapping Regulations to a Control Framework

This section presents an overview of how the major regulations and standards in this guide map to specific technology solution categories in a sample control framework.

The team mapped the five regulations and standards—SOX, GLBA, HIPAA, EUDPD, and ISO 17799—to the framework. Wherever possible, the project team conducted the mapping with the assistance of pre-existing guidance from accredited agencies and government organizations. The documents containing this guidance, which this guide refers to as *bridging documents*, are generally accepted by the audit and regulatory community as a reasonable representation of the control requirements for these regulations and standards. The team used the following bridging documents to help map the regulations to the sample control framework:

- **Sarbanes Oxley Act**. *IT Control Objectives for Sarbanes-Oxley* from the IT Governance Institute at www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=9757&TEMPLATE=/ContentManagement/ContentDisplay.cfm.
- **Gramm-Leach-Bliley Act**. *Interagency Guidelines Establishing Standards for Safeguarding Customer Information* from the Department of the Treasury; Office of the Comptroller of the Currency, Office of Thrift Supervision; Federal Reserve System, and Federal Deposit Insurance Corporation at www.ffiec.gov/ffiecinfobase/resources/info_sec/frb-sr-01-15-standards_safeguard_cus_info.pdf.
- **Health Insurance Portability and Accountability Act**. *HIPAA Administrative Simplification Regulation Text* from the Department of Health and Human Services, Office for Civil Rights at www.os.dhhs.gov/ocr/AdminSimpRegText.pdf.
- **European Union Data Protection Directive**. *Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* Official Journal L 281, 23/11/1995 P. 0031 – 0050 at http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
- **ISO/IEC 17799:2005(E) Code of Practice for Information Security Management**. Available from the International Electrotechnical Committee Web store at http://domino.iec.ch/webstore/webstore.nsf/artnum/034226.

As described in the “Caveats and Disclaimers” section, this guide does not constitute legal advice and is not a substitute for individualized legal and other advice that you should receive from your legal counsel and auditors. These mappings should therefore only be used as a general guide. To determine the specific requirements for your organization, consult your legal counsel or auditors.

Control Categories

To provide a more general overview of the compliance requirements for each of the five regulations and standards, this topic presents a high-level table of the regulations and standards that map to the control categories in the sample control framework, which is loosely based on the Microsoft Operations Framework.

The mapping in this table can help you identify which control categories apply to your organization. In addition, the table indicates where multiple regulations and standards require the same control framework categories.

IT managers can use this table to help develop a plan to address regulatory compliance requirements. For example, if your organization must comply with SOX and HIPAA, you should consider implementing controls in the categories that contain marks in the SOX and HIPAA columns. Furthermore, you might choose to prioritize your IT control efforts to focus on those control categories that many or all of the regulations require that also apply to your organization. Again, Microsoft notes that this mapping does not constitute legal advice; you must consult your legal counsel and auditors for specific, individualized guidance on this complex subject.

Table 1: Major Regulations and Standards Map to Control Categories

Control Categories	SOX	GLBA	HIPAA	EUDPD	ISO 17799
Organizational Framework	X	X	X	X	X
IT Strategic Planning	X	X	X	X	X
IT Resource Planning	X	X	X	X	X
Development and Communication of Policies and Standards	X	X	X	X	X
Solution Development	X	X	X		X
IT Risk Management	X	X	X		X
Project Management					
Change Management	X	X	X		X
Service Level Management	X	X	X	X	X
Capacity and Availability Management	X	X	X	X	X
Security Management and Administration	X	X	X	X	X
Financial Management					
Awareness and Training	X	X	X		X
Configuration Management	X		X		
Problem and Incident Management	X	X	X		X
Data Management	X	X	X	X	X
Operations Management	X		X	X	X
IT Effectiveness	X	X			X
IT Assurance	X	X	X		X
IT Compliance and Governance	X	X	X	X	X
Privacy Management		X	X	X	X

The next topic, Technology Solutions for Regulatory Compliance, presents the technology solution categories that are relevant to regulatory compliance.

Technology Solutions for Regulatory Compliance

This topic presents the technology solution categories that are relevant to regulatory compliance. So far, this guide has focused on how regulations can drive specific IT control requirements. Now the focus shifts to the technology solutions that can help address those requirements.

The team created and validated its list of technology solutions, and the categories for them that are relevant to regulatory compliance, against ISO 17799, National Institute of Standards and Technology (NIST SP800) recommendations, 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
- Incident Management and Trouble-Tracking

The next topic, Technology Solutions for IT Control, illustrates how each of the control categories in the control framework map to specific technology solutions. You can use these mappings to help determine the types of controls that you want to implement for your organization.

Technology Solutions for IT Control

The following table shows a consolidated view of the control categories. To use this table, first find the rows for the control categories that your organization needs to address. The check marks in the columns indicate which technology solutions can help you address each control category.

This next section demonstrates how specific regulations and standards drive specific technology solutions through an Applied Example. The example is based on the mappings in the previous topics in this section of the guide.

Table 2: Control Categories Mapped to Technology Solutions

	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	Physical Security	Vulnerability Identification	Monitoring and Reporting	Disaster Recovery and Failover	Incident Management and Trouble-Tracking
Organizational Framework	✓										✓							
IT Strategic Planning	✓		✓								✓	✓						
IT Resource Planning	✓		✓										✓	✓	✓			
Development and Communcation of Policies and Standards	✓																	
Solution Development	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IT Risk Management	✓		✓	✓												✓		
Project Management	✓		✓		✓						✓							
Change Management	✓		✓		✓						✓				✓			✓
Service Level Management	✓			✓													✓	
Capacity and Availability Management	✓														✓	✓	✓	✓
Security Management and Administration	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Financial Management	✓	✓	✓															
Awareness and Training	✓										✓				✓			
Configuration Management	✓				✓													
Problem and Incident Management	✓				✓										✓	✓	✓	✓
Data Management	✓											✓		✓		✓	✓	
Operations Management	✓											✓			✓		✓	
IT Effectiveness	✓																✓	
IT Assurance	✓	✓		✓							✓				✓		✓	
IT Compliance and Governance	✓	✓		✓							✓				✓		✓	
Privacy Management	✓					✓	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓

Applied Example

This topic provides a high-level overview of an applied example in which a company uses the *Regulatory Compliance Planning Guide* to understand better the processes involved when addressing regulatory compliance. The company also recognizes the benefits of using the sample control framework in the guide as an abstraction layer to define the different regulations and standards, and then determine and prioritize which technology solutions will help the company meet its regulatory compliance obligations.

Woodgrove National Bank is a financial organization with 5,000 employees that maintains its headquarters in New York. The bank is publicly traded and listed on the NYSE, and like many other financial organizations in the U.S., the bank must comply with regulations specific to the Sarbanes-Oxley Act.

Furthermore, management at the bank must also adhere to HIPAA regulations for medical and dental benefits that the bank offers its employees, and to GLBA directives because the bank is in the financial services industry.

To meet these regulatory compliance objectives, management has asked Haven Ford, the lead IT Manager for the bank, to ensure that the company's IT department passes audits that are scheduled over the next calendar year.

Haven assumes these new responsibilities with two important goals in mind:

- Achieve full compliance using IT controls whenever possible to address all of the regulations and standards that the bank currently faces.
- Minimize the time and affect that the audits have on the bank's IT department, and achieve efficiencies wherever possible toward this end based on reliable IT controls.

To achieve these goals for the bank, Haven:

1. Meets with the bank’s lawyers and auditors to discuss his goals and determine the best way forward.
2. Researches the *Regulatory Compliance Planning Guide* to determine which guidance can most readily assist him in meeting the regulatory compliance objectives for the bank.
3. Determines that a framework-based approach is good for his organization.
4. Consults Table 1, "Major Regulations and Standards Map to Control Categories," in this section to better understand the control categories that apply to the bank, specifically the columns in the table that contain references to SOX, HIPAA, and GLBA. In this example, Haven notes from the table that all three regulations that apply to Woodgrove National Bank require the Security Management and Administration control category.
5. Consults Table 2, “Control Categories Mapped to Technology Solutions”, in this section to determine any new technologies that the bank needs to focus on. Referring to this table, Haven sees that Identity Management is a technology solution category that can help with the Security Management and Administration control category.

6. Researches specific technologies in Technology Solutions for Regulatory Compliance to understand which technologies can help his team address the remaining control objectives for the bank. Haven refers to the Identity Management Solutions section for technologies that can help him improve controls for identity management and user creation for the bank. He is particularly interested in the Identity and Access Management Series of papers that the Identity Management Solutions section references. After some research, Haven decides that the guidance provided in this series would be an excellent solution for the bank's IT environment.
7. Discusses his ideas with the bank's lawyers and auditors, who help tailor his proposed plan to the bank's unique compliance needs and obligations.
8. Finalizes a plan for his team to incorporate the technology solutions on which it will focus this year to address the remaining control categories, and develop a strategy to implement them. After the plan has been reviewed and approved by the bank's lawyers and auditors, Haven allocates some of his budget to implement identity management infrastructure software at the bank.
9. Executes the finalized plan with his team.

The last topic in this section provides a Summary that reiterates the main points of this portion of the guide.

Summary

The mappings in this section show how regulations drive the need for specific IT controls in your organization. In addition, they indicate the types of technology solutions that you can use to help address the requirements for the IT controls. Finally, the authors provided an Applied Example of how to use this guide to address your organization's compliance requirements.

Technology Solutions for Regulatory Compliance

The following topics provide additional information about the technology solutions introduced in the previous section, Mapping Regulations to Technology Solutions. Each topic describes one technology solution, and then provides links to where you can get more information about the solution.

This section includes information about the following 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
- Incident Management and Trouble-Tracking

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 rsources 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.

Sybari Software

- For more information about how to protect your messaging 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.

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.

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.

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 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.

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.

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.

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.

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.

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.

Acknowledgments

The Microsoft Solutions for Security and Compliance group (MSSC) 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 this guide.

Authors

Ross Carter

John Cobb, *Wadeware LLC*

Lana Earhart

Anthony Noblett, *Socair Solutions*

Content Contributors

Don McGowan

David Mowers

Program Managers

Bill Canning

Jeff Coon, *Volt*

Editor

Jennifer Kerns, *Wadeware LLC*

Testers

Gaurav Singh Bora, *Infosys Technologies Ltd*

Archita Dash, *Infosys Technologies Ltd*

Release Manager

Karl Seng, *Siemens Agency Services*

Reviewers

Karri Alexion-Tiernan

Norman Barber

JC Cannon

Matt Clapham

Tom Daemen

Mike Danseglio

Christine Duell, *Valente Solutions*

Chris Farrow, *Configuresoft*

Joe Gimigliano, *Purdue Pharma*

Steven Hamburg, *Eclipsecurity, LLC*

Patrick Hanrion

Guy-Marie Joseph, *ConnecTalk Consulting Services*

Jason Lee

Brendon Lynch

Barney Regen, *Gaylord Entertainment*

Miles Romello, *Wachovia*

Mark Simon, *Eclipsecurity, LLC*

Ben Smith

Jeff Williams

John Wylder