
**Microsoft Solutions for Security and
Compliance**

and

**Microsoft Security Center of
Excellence**

The Security Risk Management Guide

© 2006 Microsoft Corporation. This work is licensed under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc/2.5/> or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

Contents

Chapter 1: Introduction to the Security Risk Management Guide.....	1
Executive Summary.....	1
The Environmental Challenges.....	1
A Better Way.....	1
Microsoft Role in Security Risk Management.....	1
Guide Overview	2
Critical Success Factors	2
Next Steps.....	3
Who Should Read This Guide	3
Scope of the Guide	3
Content Overview	3
Chapter 1: Introduction to the Security Risk Management Guide	3
Chapter 2: Survey of Security Risk Management Practices.....	4
Chapter 3: Security Risk Management Overview	4
Chapter 4: Assessing Risk	4
Chapter 5: Conducting Decision Support	4
Chapter 6: Implementing Controls and Measuring Program Effectiveness	5
Appendix A: Ad-Hoc Risk Assessments.....	5
Appendix B: Common Information System Assets	5
Appendix C: Common Threats	5
Appendix D: Vulnerabilities.....	5
Tools and Templates	6
Keys to Success	6
Executive Sponsorship.....	6
A Well-Defined List of Risk Management Stakeholders	7
Organizational Maturity in Terms of Risk Management.....	7
An Atmosphere of Open Communication	7
A Spirit of Teamwork.....	8
A Holistic View of the Organization.....	8
Authority Throughout the Process	8
Terms and Definitions	8
Style Conventions	10
Getting Support for This Guide.....	10
More Information	10

Chapter 2: Survey of Security Risk Management Practices	13
Comparing Approaches to Risk Management.....	13
The Reactive Approach	13
The Proactive Approach	15
Approaches to Risk Prioritization	16
Quantitative Risk Assessment.....	16
Details of the Quantitative Approach.....	17
Qualitative Risk Assessment.....	19
Comparing the Two Approaches.....	20
The Microsoft Security Risk Management Process	21
Chapter 3: Security Risk Management Overview	23
The Four Phases of the Microsoft Security Risk Management Process	23
Level of Effort	25
Laying the Foundation for the Microsoft Security Risk Management Process	25
Risk Management vs. Risk Assessment	25
Communicating Risk.....	26
Determining Your Organization's Risk Management Maturity Level	28
Organizational Risk Management Maturity Level Self Assessment	30
Defining Roles and Responsibilities.....	31
Building the Security Risk Management Team	33
Summary	34
Chapter 4: Assessing Risk.....	35
Overview.....	35
Required Inputs for the Assessing Risk Phase	36
Participants in the Assessing Risk Phase	37
Tools Provided for the Assessing Risk Phase	37
Required Output for the Assessing Risk Phase	38
Planning.....	38
Alignment	38
Scoping	38
Stakeholder Acceptance.....	39
Preparing for Success: Setting Expectations	39
Embracing Subjectivity	39
Facilitated Data Gathering	40
Data Gathering Keys to Success	40
Building Support	41
Discussing vs. Interrogating	41

Building Goodwill.....	41
Risk Discussion Preparation.....	41
Identifying Risk Assessment Inputs	41
Identifying and Classifying Assets	42
Assets.....	43
Asset Classes.....	43
Organizing Risk Information	45
Organizing by Defense-in-Depth Layers	45
Defining Threats and Vulnerabilities.....	46
Estimating Asset Exposure	47
Estimating Probability of Threats	47
Facilitating Risk Discussions	48
Meeting Preparations	48
Facilitating Discussions.....	49
Task One: Determining Organizational Assets and Scenarios	50
Task Two: Identifying Threats.....	50
Task Three: Identifying Vulnerabilities	51
Task Four: Estimating Asset Exposure	51
Task Five: Identifying Existing Controls and Probability of Exploit.....	51
Summarizing the Risk Discussion	52
Defining Impact Statements.....	52
Data Gathering Summary	53
Risk Prioritization	54
Primary Tasks and Deliverables	55
Preparing for Success.....	56
Prioritizing Security Risks.....	56
Conducting Summary Level Risk Prioritization.....	56
Conducting Detailed Level Risk Prioritization	60
Quantifying Risk	67
Task One: Assign Monetary Values to Asset Classes	68
Using Materiality for Guidance	69
Task Two: Identify the Asset Value.....	70
Task Three: Produce the Single Loss Expectancy Value (SLE)	70
Task Four: Determine the Annual Rate of Occurrence (ARO).....	71
Task Five: Determine the Annual Loss Expectancy (ALE).....	71
Summary	72
Facilitating Success in the Conducting Decision Support Phase	72

Chapter 5: Conducting Decision Support	73
Overview	73
Required Input for the Conducting Decision Support Phase	75
Participants in the Conducting Decision Support Phase	75
Tools Provided for the Conducting Decision Support Phase	76
Required Outputs for the Decision Support Phase	76
Considering the Decision Support Options	77
Accepting the Current Risk	77
Implementing Controls to Reduce Risk	78
Keys to Success	78
Building Consensus	78
Avoiding Filibusters	78
Identifying and Comparing Controls	79
Step One: Defining Functional Requirements	79
Step Two: Identifying Control Solutions	81
Organizational Controls	83
Operational Controls	84
Technological Controls	85
Step Three: Reviewing the Solution Against Requirements	86
Step Four: Estimating Risk Reduction	87
Step Five: Estimating Solution Cost	88
Acquisition Costs	89
Implementation Costs	89
Ongoing Costs	89
Communication Costs	89
Training Costs for IT Staff	89
Training Costs for Users	90
Costs to Productivity and Convenience	90
Costs for Auditing and Verifying Effectiveness	90
Step Six: Selecting the Risk Mitigation Solution	92
Summary	93
Chapter 6: Implementing Controls and Measuring Program Effectiveness	95
Overview	95
Implementing Controls	95
Required Input for the Implementing Controls Phase	96
Participants in the Implementing Controls Phase	96
Tools Provided for the Implementing Controls Phase	97

Required Outputs for the Implementing Controls Phase	97
Organizing the Control Solutions.....	97
Network Defenses	99
Host Defenses	100
Application Defenses.....	101
Data Defenses	102
Measuring Program Effectiveness	102
Required Inputs for the Measuring Program Effectiveness Phase	103
Participants in the Measuring Program Effectiveness Phase	103
Tools Provided for the Measuring Program Effectiveness Phase	104
Required Outputs for the Measuring Program Effectiveness Phase.....	104
Developing Your Organization's Security Risk Scorecard	105
Measuring Control Effectiveness	106
Reassessing New and Changed Assets and Security Risks	107
Summary	108
Conclusion to the Guide	108
Appendix A: Ad-Hoc Risk Assessments	111
Appendix B: Common Information Systems Assets.....	113
Appendix C: Common Threats	117
Appendix D: Vulnerabilities.....	119
Acknowledgments.....	121

Chapter 1: Introduction to the Security Risk Management Guide

Executive Summary

The Environmental Challenges

Most organizations recognize the critical role that information technology (IT) plays in supporting their business objectives. But today's highly connected IT infrastructures exist in an environment that is increasingly hostile—attacks are being mounted with increasing frequency and are demanding ever shorter reaction times. Often, organizations are unable to react to new security threats before their business is impacted. Managing the security of their infrastructures—and the business value that those infrastructures deliver—has become a primary concern for IT departments.

Furthermore, new legislation that stems from privacy concerns, financial obligations, and corporate governance is forcing organizations to manage their IT infrastructures more closely and effectively than in the past. Many government agencies and organizations that do business with those agencies are mandated by law to maintain a minimum level of security oversight. Failure to proactively manage security may put executives and whole organizations at risk due to breaches in fiduciary and legal responsibilities.

A Better Way

The Microsoft approach to security risk management provides a proactive approach that can assist organizations of all sizes with their response to the requirements presented by these environmental and legal challenges. A formal security risk management process enables enterprises to operate in the most cost efficient manner with a known and acceptable level of business risk. It also gives organizations a consistent, clear path to organize and prioritize limited resources in order to manage risk. You will realize the benefits of using security risk management when you implement cost-effective controls that lower risk to an acceptable level.

The definition of acceptable risk, and the approach to manage risk, varies for every organization. There is no right or wrong answer; there are many risk management models in use today. Each model has tradeoffs that balance accuracy, resources, time, complexity, and subjectivity. Investing in a risk management process—with a solid framework and clearly defined roles and responsibilities—prepares the organization to articulate priorities, plan to mitigate threats, and address the next threat or vulnerability to the business. Additionally, an effective risk management program will help the company to make significant progress toward meeting new legislative requirements.

Microsoft Role in Security Risk Management

This is the first prescriptive guide that Microsoft has published that focuses entirely on security risk management. Based on both Microsoft experiences and those of its

customers, this guidance was tested and reviewed by customers, partners, and technical reviewers during development. The goal of this effort is to deliver clear, actionable guidance on how to implement a security risk management process that delivers a number of benefits, including:

- Moving customers to a proactive security posture and freeing them from a reactive, frustrating process.
- Making security measurable by showing the value of security projects.
- Helping customers to efficiently mitigate the largest risks in their environments rather than applying scarce resources to all possible risks.

Guide Overview

This guide uses industry standards to deliver a hybrid of established risk management models in an iterative four-phase process that seeks to balance cost and effectiveness. During a risk assessment process, qualitative steps identify the most important risks quickly. A quantitative process based on carefully defined roles and responsibilities follows next. This approach is very detailed and leads to a thorough understanding of the most important risks. Together, the qualitative and quantitative steps in the risk assessment process provide the basis on which you can make solid decisions about risk and mitigation, following an intelligent business process.

Note Do not worry if some of the concepts that this executive summary discusses are new to you; subsequent chapters explain them in detail. For example, Chapter 2, "Survey of Security Risk Management Practices," examines the differences between qualitative and quantitative approaches to risk assessment.

The Microsoft security risk management process enables organizations to implement and maintain processes to identify and prioritize risks in their IT environments. Moving customers from a reactive focus to a proactive focus fundamentally improves security within their environments. In turn, improved security facilitates increased availability of IT infrastructures and improved business value.

The Microsoft security risk management process offers a combination of various approaches including pure quantitative analysis, return on security investment (ROSI) analysis, qualitative analysis, and best practice approaches. It is important to note that this guide addresses a process and has no specific technology requirements.

Critical Success Factors

There are many keys to successful implementation of a security risk management program throughout an organization. Several of those are particularly critical and will be presented here; others are discussed in the "Keys to Success" section that appears later in this chapter.

First, security risk management will fail without executive support and commitment. When security risk management is led from the top, organizations can articulate security in terms of value to the business. Next, a clear definition of roles and responsibilities is fundamental to success. Business owners are responsible for identifying the impact of a risk. They are also in the best position to articulate the business value of assets that are necessary to operate their functions. The Information Security Group owns identifying the probability that the risk will occur by taking current and proposed controls into account. The Information Technology group is responsible for implementing controls that the Security Steering Committee has selected when the probability of an exploit presents an unacceptable risk.

Next Steps

Investing in a security risk management program—with a solid, achievable process and defined roles and responsibilities—prepares an organization to articulate priorities, plan to mitigate threats, and address critical business threats and vulnerabilities. Use this guide to evaluate your preparedness and to guide your security risk management capabilities. If you require or would like greater assistance, contact a Microsoft account team or Microsoft Services partner.

Who Should Read This Guide

This guide is primarily intended for consultants, security specialists, systems architects, and IT professionals who are responsible for planning application or infrastructure development and deployment across multiple projects. These roles include the following common job descriptions:

- Architects and planners who are responsible for driving the architecture efforts for their organizations
- Members of the information security team who are focused purely on providing security across platforms within an organization
- Security and IT auditors who are accountable for ensuring that organizations have taken suitable precautions to protect their significant business assets
- Senior executives, business analysts, and Business Decision Makers (BDMs) who have critical business objectives and requirements that need IT support
- Consultants and partners who need knowledge transfer tools for enterprise customers and partners

Scope of the Guide

This guide is focused on how to plan, establish, and maintain a successful security risk management process in organizations of all sizes and types. The material explains how to conduct each phase of a risk management project and how to turn the project into an ongoing process that drives the organization toward the most useful and cost effective controls to mitigate security risks.

Content Overview

The Security Risk Management Guide comprises six chapters, described below briefly. Each chapter builds on the end-to-end practice required to effectively initiate and operate an ongoing security risk management process in your organization. Following the chapters are several appendices and tools to help organize your security risk management projects.

Chapter 1: Introduction to the Security Risk Management Guide

This chapter introduces the guide and provides a brief overview of each chapter.

Chapter 2: Survey of Security Risk Management Practices

It is important to lay a foundation for the Microsoft security risk management process by reviewing the different ways that organizations have approached security risk management in the past. Readers who are already well versed in security risk management may want to skim through the chapter quickly; others who are relatively new to security or risk management are encouraged to read it thoroughly. The chapter starts with a review of the strengths and weaknesses of the proactive and reactive approaches to risk management. It then revisits in detail the concept that Chapter 1, "Introduction to the Security Risk Management Guide," introduces of organizational risk management maturity. Finally, the chapter assesses and compares qualitative risk management and quantitative risk management, the two traditional methods. The process is presented as an alternative method, one that provides a balance between these methodologies, resulting in a process that has proven to be effective within Microsoft.

Chapter 3: Security Risk Management Overview

This chapter provides a more detailed look at the Microsoft security risk management process and introduces some of the important concepts and keys to success. It also provides advice on how to prepare for the process by using effective planning and building a strong Security Risk Management Team with well defined roles and responsibilities.

Chapter 4: Assessing Risk

This chapter explains the Assessing Risk phase of the Microsoft security risk management process in detail. Steps in this phase include planning, facilitated data gathering, and risk prioritization. The risk assessment process consists of multiple tasks, some of which can be quite demanding for a large organization. For example, identifying and determining values of business assets may take a lot of time. Other tasks such as identifying threats and vulnerabilities require a lot of technical expertise. The challenges related to these tasks illustrate the importance of proper planning and building a solid Security Risk Management Team, as Chapter 3, "Security Risk Management Overview," emphasizes.

In the summary risk prioritization, the Security Risk Management Team uses a qualitative approach to triage the full list of security risks so that it can quickly identify the most significant ones for further analysis. The top risks are then subjected to a detailed analysis using quantitative techniques. This results in a short list of the most significant risks with detailed metrics that the team can use to make sensible decisions during the next phase of the process.

Chapter 5: Conducting Decision Support

During the Conducting Decision Support phase of the process, the Security Risk Management Team determines how to address the key risks in the most effective and cost efficient manner. The team identifies controls; determines costs associated with acquiring, implementing, and supporting each control; assesses the degree of risk reduction that each control achieves; and, finally, works with the Security Steering Committee to determine which controls to implement. The end result is a clear and actionable plan to control or accept each of the top risks identified in the Assessing Risk phase.

Chapter 6: Implementing Controls and Measuring Program Effectiveness

This chapter covers the last two phases of the Microsoft security risk management process: Implementing Controls and Measuring Program Effectiveness. The Implementing Controls phase is self-explanatory: The mitigation owners create and execute plans based on the list of control solutions that emerged during the decision support process to mitigate the risks identified in the Assessing Risk phase. The chapter provides links to prescriptive guidance that your organization's mitigation owners may find helpful for addressing a variety of risks. The Measuring Program Effectiveness phase is an ongoing one in which the Security Risk Management team periodically verifies that the controls implemented during the preceding phase are actually providing the expected degree of protection.

Another step of this phase is estimating the overall progress that the organization is making with regard to security risk management as a whole. The chapter introduces the concept of a "Security Risk Scorecard" that you can use to track how your organization is performing. Finally, the chapter explains the importance of watching for changes in the computing environment such as the addition or removal of systems and applications or the appearance of new threats and vulnerabilities. These types of changes may require prompt action by the organization to protect itself from new or changing risks.

Appendix A: Ad-Hoc Risk Assessments

This appendix contrasts the formal enterprise risk assessment process with the ad-hoc approach that many organizations take. It highlights the advantages and disadvantages of each method and suggests when it makes the most sense to use one or the other.

Appendix B: Common Information System Assets

This appendix lists information system assets commonly found in organizations of various types. It is not intended to be comprehensive, and it is unlikely that this list will represent all of the assets present in your organization's unique environment. Therefore, it is important that you customize the list during the risk assessment process. It is provided as a reference list and a starting point to help your organization get started.

Appendix C: Common Threats

This appendix lists threats likely to affect a wide variety of organizations. The list is not comprehensive, and, because it is static, will not remain current. Therefore, it is important that you remove threats that are not relevant to your organization and add newly identified ones to it during the assessment phase of your project. It is provided as a reference list and a starting point to help your organization get started.

Appendix D: Vulnerabilities

This appendix lists vulnerabilities likely to affect a wide variety of organizations. The list is not comprehensive, and, because it is static, will not remain current. Therefore, it is important that you remove vulnerabilities that are not relevant to your organization and add newly identified ones to it during the risk assessment process. It is provided as a reference list and a starting point to help your organization get started.

Tools and Templates

A collection of tools and templates are included with this guide to make it easier for your organization to implement the Microsoft security risk management process. These tools and templates are included in a Windows Installer file called *Security Risk Management Guide Tools and Templates.msi*, which is available on the Download Center. When you run the *Security Risk Management Guide Tools and Templates.msi* file, the following folder will be created in the default location:

- **%USERPROFILE%\My Documents\Security Risk Management Guide Tools and Templates.** This folder contains the following Tools and Templates:
 - Data Gathering Template (SRMGTool1-Data Gathering Tool.doc). You can use this template in the Assessing Risk phase during the workshops that Chapter 4, "Assessing Risk," describes.
 - Summary Level Risk Analysis Worksheet (SRMGTool2-Summary Risk Level.xls). This Microsoft® Excel® worksheet will help your organization to conduct the first pass of risk analysis: the summary level analysis.
 - Detail Level Risk Analysis Worksheet (SRMGTool3-Detailed Level Risk Prioritization.xls). This Excel worksheet will help your organization to conduct a more exhaustive analysis of the top risks identified during the summary level analysis.
 - Sample Schedule (SRMGTool4-Sample Project Schedule.xls). This Excel worksheet shows a high-level project schedule for the Microsoft security risk management process. It includes the phases, steps, and tasks discussed throughout the guide.

Keys to Success

Whenever an organization undertakes a major new initiative, various foundational elements must be in place if the effort is to be successful. Microsoft has identified components that must be in place prior to the implementation of a successful security risk management process and that must remain in place once it is underway. They are:

- Executive sponsorship.
- A well-defined list of risk management stakeholders.
- Organizational maturity in terms of risk management.
- An atmosphere of open communication.
- A spirit of teamwork.
- A holistic view of the organization.
- Authority throughout the process.

The following sections discuss these elements that are required throughout the entire security risk management process; additional ones relevant only to specific phases are highlighted in the chapters that discuss those phases.

Executive Sponsorship

Senior management must unambiguously and enthusiastically support the security risk management process. Without this sponsorship, stakeholders may resist or undermine efforts to use risk management to make the organization more secure. Additionally, without clear executive sponsorship, individual employees may disregard directives for

how to perform their jobs or help to protect organizational assets. There are many possible reasons why employees may fail to cooperate. Among them is a generalized resistance to change; a lack of appreciation for the importance of effective security risk management; an inaccurate belief that they as individuals have a solid understanding of how to protect business assets even though their point of view may not be as broad and deep as that of the Security Risk Management Team; or the belief that their part of the organization would never be targeted by potential attackers.

Sponsorship implies the following:

- Delegation of authority and responsibility for a clearly articulated project scope to the Security Risk Management Team
- Support for participation by all staff as needed
- Allocation of sufficient resources such as personnel and financial resources
- Unambiguous and energetic support of the security risk management process
- Participation in the review of the findings and recommendations of the security risk management process

A Well-Defined List of Risk Management Stakeholders

This guide frequently discusses stakeholders, which in this context means members of the organization with a vested interest in the results of the security risk management process. The Security Risk Management Team needs to understand who all of the stakeholders are—this includes the core team itself as well as the executive sponsor(s). It will also include the people who own the business assets that are to be evaluated. The IT personnel responsible and accountable for designing, deploying, and managing the business assets are also key stakeholders.

The stakeholders must be identified so that they can then join the security risk management process. The Security Risk Management Team must invest time in helping these people to understand the process and how it can help them to protect their assets and save money in the long term.

Organizational Maturity in Terms of Risk Management

If an organization currently has no security risk management process in place, the Microsoft security risk management process may involve too much change in order to implement it in its entirety, all at once. Even if an organization has some informal processes, such as ad-hoc efforts that are launched in response to specific security issues, the process may seem overwhelming. However, it can be effective in organizations with more maturity in terms of risk management; maturity is evidenced by such things as well defined security processes and a solid understanding and acceptance of security risk management at many levels of the organization. Chapter 3, "Security Risk Management Overview," discusses the concept of security risk management maturity and how to calculate your organization's maturity level.

An Atmosphere of Open Communication

Many organizations and projects operate purely on a need-to-know basis, which frequently leads to misunderstandings and impairs the ability of a team to deliver a successful solution. The Microsoft security risk management process requires an open

and honest approach to communications, both within the team and with key stakeholders. A free-flow of information not only reduces the risk of misunderstandings and wasted effort but also ensures that all team members can contribute to reducing uncertainties surrounding the project. Open, honest discussion about what risks have been identified and what controls might effectively mitigate those risks is critical to the success of the process.

A Spirit of Teamwork

The strength and vitality of the relationships among all of the people working on the Microsoft security risk management process will greatly affect the effort. Regardless of the support from senior management, the relationships that are developed among security staff and management and the rest of the organization are critical to the overall success of the process. It is extremely important that the Security Risk Management Team fosters a spirit of teamwork with each of the representatives from the various business units with which they work throughout the project. The team can facilitate this by effectively demonstrating the business value of security risk management to individual managers from those business units and by showing staff members how in the long run the project might make it easier for them to do their jobs effectively.

A Holistic View of the Organization

All participants involved in the Microsoft security risk management process, particularly the Security Risk Management Team, need to consider the entire organization during their work. What is best for one particular employee is frequently not what is best for the organization as a whole. Likewise, what is most beneficial to one business unit may not be in the best interest of the organization. Staff and managers from a particular business unit will instinctively seek to drive the process toward outcomes that will benefit them and their parts of the organization.

Authority Throughout the Process

Participants in the Microsoft security risk management process accept responsibility for identifying and controlling the most significant security risks to the organization. In order to effectively mitigate those risks by implementing sensible controls, they will also require sufficient authority to make the appropriate changes. Team members must be empowered to meet the commitments assigned to them. Empowerment requires that team members are given the resources necessary to perform their work, are responsible for the decisions that affect their work, and understand the limits to their authority and the escalation paths available to handle issues that transcend these limits.

Terms and Definitions

Terminology related to security risk management can sometimes be difficult to understand. At other times, an easily recognized term may be interpreted differently by different people. For these reasons it is important that you understand the definitions that the authors of this guide used for important terms that appear throughout it. Many of the definitions provided below originated in documents published by two other organizations: the International Standards Organization (ISO) and the Internet Engineering Task Force (IETF). Web addresses for those organizations are provided in the "More Information" section later in this chapter. The following list provides a consolidated view of the key components of security risk management:

- **Annual Loss Expectancy (ALE).** The total amount of money that an organization will lose in one year if nothing is done to mitigate a risk.
- **Annual Rate of Occurrence (ARO).** The number of times that a risk is expected to occur during one year.
- **Asset.** Anything of value to an organization, such as hardware and software components, data, people, and documentation.
- **Availability.** The property of a system or a system resource that ensures that it is accessible and usable upon demand by an authorized system user. Availability is one of the core characteristics of a secure system.
- **CIA.** See Confidentiality, Integrity, and Availability.
- **Confidentiality.** The property that information is not made available or disclosed to unauthorized individuals, entities, or processes (ISO 7498-2).
- **Control.** An organizational, procedural, or technological means of managing risk; a synonym for safeguard or countermeasure.
- **Cost-benefit analysis.** An estimate and comparison of the relative value and cost associated with each proposed control so that the most effective are implemented.
- **Decision support.** Prioritization of risk based on a cost-benefit analysis. The cost for the security solution to mitigate a risk is weighed against the business benefit of mitigating the risk.
- **Defense-in-depth.** The approach of using multiple layers of security to guard against failure of a single security component.
- **Exploit.** A means of using a vulnerability in order to cause a compromise of business activities or information security.
- **Exposure.** A threat action whereby sensitive data is directly released to an unauthorized entity (RFC 2828). The Microsoft security risk management process narrows this definition to focus on the extent of damage to a business asset.
- **Impact.** The overall business loss expected when a threat exploits a vulnerability against an asset.
- **Integrity.** The property that data has not been altered or destroyed in an unauthorized manner (ISO 7498-2).
- **Mitigation.** Addressing a risk by taking actions designed to counter the underlying threat.
- **Mitigation solution.** The implementation of a control, which is the organizational, procedural, or technological control put into place to manage a security risk.
- **Probability.** The likelihood that an event will occur.
- **Qualitative risk management.** An approach to risk management in which the participants assign relative values to the assets, risks, controls, and impacts.
- **Quantitative risk management.** An approach to risk management in which participants attempt to assign objective numeric values (for example, monetary values) to the assets, risks, controls, and impacts.
- **Reputation.** The opinion that people hold about an organization; most organizations' reputations have real value even though they are intangible and difficult to calculate.
- **Return On Security Investment (ROSI).** The total amount of money that an organization is expected to save in a year by implementing a security control.
- **Risk.** The combination of the probability of an event and its consequence. (ISO Guide 73).

- **Risk assessment.** The process by which risks are identified and the impact of those risks determined.
- **Risk management.** The process of determining an acceptable level of risk, assessing the current level of risk, taking steps to reduce risk to the acceptable level, and maintaining that level of risk.
- **Single Loss Expectancy (SLE).** The total amount of revenue that is lost from a single occurrence of a risk.
- **Threat.** A potential cause of an unwanted impact to a system or organization. (ISO 13335-1).
- **Vulnerability.** Any weakness, administrative process, or act or physical exposure that makes an information asset susceptible to exploit by a threat.

Style Conventions

This guide uses the following style conventions and terminology.

Element	Meaning
Note	Alerts the reader to supplementary information.
Woodgrove example	Alerts the reader that the content is related to the fictitious example company, "Woodgrove Bank."

Getting Support for This Guide

This guide seeks to clearly describe a process that organizations can follow to implement and maintain a security risk management program. If you need assistance in implementing a risk management program, you should contact your Microsoft account team. There is no phone support available for this document.

Feedback or questions on this guide may be addressed to secwish@microsoft.com.

More Information

The following information sources were the latest available on topics closely related to security risk management at the time that this guide was published.

The Microsoft Operations Framework (MOF) provides guidance that enables organizations to achieve mission-critical system reliability, availability, supportability, and manageability of Microsoft products and technologies. MOF provides operational guidance in the form of white papers, operations guides, assessment tools, best practices, case studies, templates, support tools, and services. This guidance addresses the people, process, technology, and management issues pertaining to complex, distributed, and heterogeneous IT environments. More information about [MOF](https://www.microsoft.com/mof) is available at www.microsoft.com/mof.

The Microsoft Solutions Framework (MSF) may help you successfully execute the action plans created as part of the Microsoft security risk management process. Designed to help organizations deliver high quality technology solutions on time and on budget, MSF is a deliberate and disciplined approach to technology projects and is based on a defined set of principles, models, disciplines, concepts, guidelines, and proven practices from Microsoft. For more information on [MSF](https://www.microsoft.com/msf), see www.microsoft.com/msf.

The Microsoft Security Center is an exhaustive and well-organized collection of documentation addressing a wide range of security topics. The [Security Center](https://www.microsoft.com/security/guidance/default.aspx) is available at www.microsoft.com/security/guidance/default.aspx.

The Microsoft Windows 2000 Server Solution for Security is a prescriptive solution aimed at helping to reduce security vulnerabilities and lowering the costs of exposure and security management in Microsoft Windows® 2000 environments. Chapters 2, 3, and 4 of the Microsoft Windows 2000 Server Solution for Security guide comprise the first security risk management guidance that Microsoft published, which was referred to as the Security Risk Management Discipline (SRMD). The guide you are reading serves as a replacement for the security risk management content in the Microsoft Windows 2000 Server Solution for Security guide. The [Microsoft Solution for Securing Windows 2000 Server guide](http://go.microsoft.com/fwlink/?LinkId=14837) is available at <http://go.microsoft.com/fwlink/?LinkId=14837>.

The National Institute for Standards and Technology (NIST) offers an excellent guide on risk management. The [Risk Management Guide for Information Technology Systems](http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf) (July 2002) is available at <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.

NIST also offers a guide on performing a security assessment of your own organization. The [Security Self-Assessment Guide for Information Technology Systems](http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf) (November 2001) is available at <http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>.

The ISO offers a high-level code of practice known as the *Information technology—Code of practice for information security management*, or [ISO 17799](https://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3=). It is available for a fee at www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3=.

The ISO has published a variety of [other standards documents](https://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3=), some of which are referred to within this guide. They are available for a fee at www.iso.org.

The Computer Emergency Response Team (CERT), located in the Software Engineering Institute at Carnegie-Mellon University, has created OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM), a self-directed risk assessment and planning technique. More information about [OCTAVE](https://www.cert.org/octave) is available online at www.cert.org/octave.

Control Objectives for Information and Related Technology (COBIT) offers generally applicable and accepted standards for good IT security and control practices that provide a reference framework for management, users, and IS audit, control, and security practitioners. [COBIT](https://www.isaca.org/cobit) is available online for a fee from the Information Systems Audit and Control Association (ISACA) at www.isaca.org/cobit.

The IETF has published [Request for Comments \(RFC\) 2828](https://www.faqs.org/rfcs/rfc2828), which is a publicly available memo called the Internet Security Glossary which provides standard definitions for a large number of information system security terms. It is available at www.faqs.org/rfcs/rfc2828.html.

Chapter 2: Survey of Security Risk Management Practices

This chapter starts with a review of the strengths and weaknesses of the proactive and reactive approaches to security risk management. The chapter then assesses and compares qualitative security risk management and quantitative security risk management, the two traditional methods. The Microsoft security risk management process is presented as an alternative method, one that provides a balance between these methodologies, resulting in a process that has proven to be extremely effective within Microsoft.

Note It is important to lay a foundation for the Microsoft security risk management process by reviewing the different ways that organizations have approached security risk management in the past. Readers who are already well versed in security risk management may want to skim through the chapter quickly; others who are relatively new to security or risk management are encouraged to read it thoroughly.

Comparing Approaches to Risk Management

Many organizations are introduced to security risk management by the necessity of responding to a relatively small security incident. A staff member's computer becomes infected with a virus, for example, and an office-manager-turned-in-house-PC-expert must figure out how to eradicate the virus without destroying the computer or the data that it held. Whatever the initial incident, as more and more issues relating to security arise and begin to impact the business, many organizations get frustrated with responding to one crisis after another. They want an alternative to this reactive approach, one that seeks to reduce the probability that security incidents will occur in the first place. Organizations that effectively manage risk evolve toward a more proactive approach, but as you will learn in this chapter, it is only part of the solution.

The Reactive Approach

Today, many information technology (IT) professionals feel tremendous pressure to complete their tasks quickly with as little inconvenience to users as possible. When a security event occurs, many IT professionals feel like the only things they have time to do are to contain the situation, figure out what happened, and fix the affected systems as quickly as possible. Some may try to identify the root cause, but even that might seem like a luxury for those under extreme resource constraints. While a reactive approach can be an effective tactical response to security risks that have been exploited and turned into security incidents, imposing a small degree of rigor to the reactive approach can help organizations of all types to better use their resources.

Recent security incidents may help an organization to predict and prepare for future problems. This means that an organization that takes time to respond to security incidents in a calm and rational manner while determining the underlying reasons that allowed the incident to transpire will be better able to both protect itself from similar problems in the future and respond more quickly to other issues that may arise.

A deep examination into incident response is beyond the scope of this guide, but following six steps when you respond to security incidents can help you manage them quickly and efficiently:

1. **Protect human life and people's safety.** This should always be your first priority. For example, if affected computers include life support systems, shutting them off may not be an option; perhaps you could logically isolate the systems on the network by reconfiguring routers and switches without disrupting their ability to help patients.
2. **Contain the damage.** Containing the harm that the attack caused helps to limit additional damage. Protect important data, software, and hardware quickly. Minimizing disruption of computing resources is an important consideration, but keeping systems up during an attack may result in greater and more widespread problems in the long run. For example, if you contract a worm in your environment, you could try to limit the damage by disconnecting servers from the network. However, sometimes disconnecting servers can cause more harm than good. Use your best judgment and your knowledge of your own network and systems to make this determination. If you determine that there will be no adverse effects, or that they would be outweighed by the positive benefits of activity, containment should begin as quickly as possible during a security incident by disconnecting from the network the systems known to be affected. If you cannot contain the damage by isolating the servers, ensure that you actively monitor the attacker's actions in order to be able to remedy the damage as soon as possible. And in any event, ensure that all log files are saved before shutting off any server, in order to preserve the information contained in those files as evidence if you (or your lawyers) need it later.
3. **Assess the damage.** Immediately make a duplicate of the hard disks in any servers that were attacked and put those aside for forensic use later. Then assess the damage. You should begin to determine the extent of the damage that the attack caused as soon as possible, right after you contain the situation and duplicate the hard disks. This is important so that you can restore the organization's operations as soon as possible while preserving a copy of the hard disks for investigative purposes. If it is not possible to assess the damage in a timely manner, you should implement a contingency plan so that normal business operations and productivity can continue. It is at this point that organizations may want to engage law enforcement regarding the incident; however, you should establish and maintain working relationships with law enforcement agencies that have jurisdiction over your organization's business before an incident occurs so that when a serious problem arises you know whom to contact and how to work with them. You should also advise your company's legal department immediately, so that they can determine whether a civil lawsuit can be brought against anyone as a result of the damage.
4. **Determine the cause of the damage.** In order to ascertain the origin of the assault, it is necessary to understand the resources at which the attack was aimed and what vulnerabilities were exploited to gain access or disrupt services. Review the system configuration, patch level, system logs, audit logs, and audit trails on both the systems that were directly affected as well as network devices that route traffic to them. These reviews often help you to discover where the attack originated in the system and what other resources were affected. You should conduct this activity on the computer systems in place and not on the backed up drives created in step 3. Those drives must be preserved intact for forensic purposes so that law enforcement or your lawyers can use them to trace the perpetrators of the attack and bring them to justice. If you need to create a backup for testing purposes to determine the cause of the damage, create a second backup from your original system and leave the drives created in step 3 unused.
5. **Repair the damage.** In most cases, it is very important that the damage be repaired as quickly as possible to restore normal business operations and recover data lost during the attack. The organization's business continuity plans and procedures should cover the restoration strategy. The incident response team should also be available to handle the restore and recovery process or to provide guidance on the

process to the responsible team. During recovery, contingency procedures are executed to limit the spread of the damage and isolate it. Before returning repaired systems to service be careful that they are not reinfected immediately by ensuring that you have mitigated whatever vulnerabilities were exploited during the incident.

6. **Review response and update policies.** After the documentation and recovery phases are complete, you should review the process thoroughly. Determine with your team the steps that were executed successfully and what mistakes were made. In almost all cases, you will find that your processes need to be modified to allow you to handle incidents better in the future. You will inevitably find weaknesses in your incident response plan. This is the point of this after-the-fact exercise—you are looking for opportunities for improvement. Any flaws should prompt another round of the incident-response planning process so that you can handle future incidents more smoothly.

This methodology is illustrated in the following diagram:

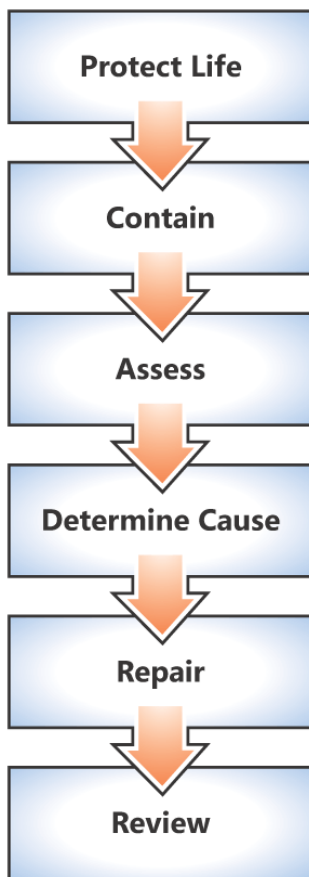


Figure 2.1: Incident Response Process

The Proactive Approach

Proactive security risk management has many advantages over a reactive approach. Instead of waiting for bad things to happen and then responding to them afterwards, you minimize the possibility of the bad things ever occurring in the first place. You make plans to protect your organization's important assets by implementing controls that reduce the risk of vulnerabilities being exploited by malicious software, attackers, or accidental misuse. An analogy may help to illustrate this idea. Influenza is a deadly respiratory disease that infects millions of people in the United States alone each year. Of those,

over 100,000 must be treated in hospitals, and about 36,000 die. You could choose to deal with the threat of the disease by waiting to see if you get infected and then taking medicine to treat the symptoms if you do become ill. Alternatively, you could choose to get vaccinated before the influenza season begins.

Organizations should not, of course, completely forsake incident response. An effective proactive approach can help organizations to significantly reduce the number of security incidents that arise in the future, but it is not likely that such problems will completely disappear. Therefore, organizations should continue to improve their incident response processes while simultaneously developing long-term proactive approaches.

Later sections in this chapter, and the remaining chapters of this guide, will examine proactive security risk management in detail. Each of the security risk management methodologies shares some common high-level procedures:

1. Identify business assets.
2. Determine what damage an attack against an asset could cause to the organization.
3. Identify the security vulnerabilities that the attack could exploit.
4. Determine how to minimize the risk of attack by implementing appropriate controls.

Approaches to Risk Prioritization

The terms *risk management* and *risk assessment* are used frequently throughout this guide, and, although related, they are not interchangeable. The Microsoft security risk management process defines risk management as the overall effort to manage risk to an acceptable level across the business. Risk assessment is defined as the process to identify and prioritize risks to the business.

There are many different methodologies for prioritizing or assessing risks, but most are based on one of two approaches or a combination of the two: quantitative risk management or qualitative risk management. Refer to the list of resources in the "More Information" section at the end of Chapter 1, "Introduction to the Security Risk Management Guide," for links to some other risk assessment methodologies. The next few sections of this chapter are a summary and comparison of quantitative risk assessment and qualitative risk assessment, followed by a brief description of the Microsoft security risk management process so that you can see how it combines aspects of both approaches.

Quantitative Risk Assessment

In quantitative risk assessments, the goal is to try to calculate objective numeric values for each of the components gathered during the risk assessment and cost-benefit analysis. For example, you estimate the true value of each business asset in terms of what it would cost to replace it, what it would cost in terms of lost productivity, what it would cost in terms of brand reputation, and other direct and indirect business values. You endeavor to use the same objectivity when computing asset exposure, cost of controls, and all of the other values that you identify during the risk management process.

Note This section is intended to show at a high level some of the steps involved in quantitative risk assessments; it is not a prescriptive guide for using that approach in security risk management projects.

There are some significant weaknesses inherent in this approach that are not easily overcome. First, there is no formal and rigorous way to effectively calculate values for assets and controls. In other words, while it may appear to give you more detail, the financial values actually obscure the fact that the numbers are based on estimates. How

can you precisely and accurately calculate the impact that a highly public security incident might have on your brand? If it is available you can examine historical data, but quite often it is not.

Second, organizations that have tried to meticulously apply all aspects of quantitative risk management have found the process to be extremely costly. Such projects usually take a very long time to complete their first full cycle, and they usually involve a lot of staff members arguing over the details of how specific fiscal values were calculated. Third, for organizations with high value assets, the cost of exposure may be so high that you would spend an exceedingly large amount of money to mitigate any risks to which you were exposed. This is not realistic, though; an organization would not spend its entire budget to protect a single asset, or even its top five assets.

Details of the Quantitative Approach

At this point, it may be helpful to gain a general understanding of both the advantages and drawbacks of quantitative risk assessments. The rest of this section looks at some of the factors and values that are typically evaluated during a quantitative risk assessment such as asset valuation; costing controls; determining Return On Security Investment (ROSI); and calculating values for Single Loss Expectancy (SLE), Annual Rate of Occurrence (ARO), and Annual Loss Expectancy (ALE). This is by no means a comprehensive examination of all aspects of quantitative risk assessment, merely a brief examination of some of the details of that approach so that you can see that the numbers that form the foundation of all the calculations are themselves subjective.

Valuing Assets

Determining the monetary value of an asset is an important part of security risk management. Business managers often rely on the value of an asset to guide them in determining how much money and time they should spend securing it. Many organizations maintain a list of asset values (AVs) as part of their business continuity plans. Note how the numbers calculated are actually subjective estimates, though: No objective tools or methods for determining the value of an asset exist. To assign a value to an asset, calculate the following three primary factors:

- **The overall value of the asset to your organization.** Calculate or estimate the asset's value in direct financial terms. Consider a simplified example of the impact of temporary disruption of an e-commerce Web site that normally runs seven days a week, 24 hours a day, generating an average of \$2,000 per hour in revenue from customer orders. You can state with confidence that the annual value of the Web site in terms of sales revenue is \$17,520,000.
- **The immediate financial impact of losing the asset.** If you deliberately simplify the example and assume that the Web site generates a constant rate per hour, and the same Web site becomes unavailable for six hours, the calculated exposure is .000685 or .0685 percent per year. By multiplying this exposure percentage by the annual value of the asset, you can predict that the directly attributable losses in this case would be approximately \$12,000. In reality, most e-commerce Web sites generate revenue at a wide range of rates depending upon the time of day, the day of the week, the season, marketing campaigns, and other factors. Additionally, some customers may find an alternative Web site that they prefer to the original, so the Web site may have some permanent loss of users. Calculating the revenue loss is actually quite complex if you want to be precise and consider all potential types of loss.
- **The indirect business impact of losing the asset.** In this example, the company estimates that it would spend \$10,000 on advertising to counteract the negative publicity from such an incident. Additionally, the company also estimates a loss of .01 or 1 percent of annual sales, or \$175,200. By combining the extra advertising

expenses and the loss in annual sales revenue, you can predict a total of \$185,200 in indirect losses in this case.

Determining the SLE

The SLE is the total amount of revenue that is lost from a single occurrence of the risk. It is a monetary amount that is assigned to a single event that represents the company's potential loss amount if a specific threat exploits a vulnerability. (The SLE is similar to the impact of a qualitative risk analysis.) Calculate the SLE by multiplying the asset value by the exposure factor (EF). The exposure factor represents the percentage of loss that a realized threat could have on a certain asset. If a Web farm has an asset value of \$150,000, and a fire results in damages worth an estimated 25 percent of its value, then the SLE in this case would be \$37,500. This is an oversimplified example, though; other expenses may need to be considered.

Determining the ARO

The ARO is the number of times that you reasonably expect the risk to occur during one year. Making these estimates is very difficult; there is very little actuarial data available. What has been gathered so far appears to be private information held by a few property insurance firms. To estimate the ARO, draw on your past experience and consult security risk management experts and security and business consultants. The ARO is similar to the probability of a qualitative risk analysis, and its range extends from 0 percent (never) to 100 percent (always).

Determining the ALE

The ALE is the total amount of money that your organization will lose in one year if nothing is done to mitigate the risk. Calculate this value by multiplying the SLE by the ARO. The ALE is similar to the relative rank of a qualitative risk analysis.

For example, if a fire at the same company's Web farm results in \$37,500 in damages, and the probability, or ARO, of a fire taking place has an ARO value of 0.1 (indicating once in ten years), then the ALE value in this case would be \$3,750 ($\$37,500 \times 0.1 = \$3,750$).

The ALE provides a value that your organization can work with to budget what it will cost to establish controls or safeguards to prevent this type of damage—in this case, \$3,750 or less per year—and provide an adequate level of protection. It is important to quantify the real possibility of a risk and how much damage, in monetary terms, the threat may cause in order to be able to know how much can be spent to protect against the potential consequence of the threat.

Determining Cost of Controls

Determining the cost of controls requires accurate estimates on how much acquiring, testing, deploying, operating, and maintaining each control would cost. Such costs would include buying or developing the control solution; deploying and configuring the control solution; maintaining the control solution; communicating new policies or procedures related to the new control to users; training users and IT staff on how to use and support the control; monitoring the control; and contending with the loss of convenience or productivity that the control might impose. For example, to reduce the risk of fire damaging the Web farm, the fictional organization might consider deploying an automated fire suppression system. It would need to hire a contractor to design and install the system and would then need to monitor the system on an ongoing basis. It would also need to check the system periodically and, occasionally, recharge it with whatever chemical retardants the system uses.

ROSI

Estimate the cost of controls by using the following equation:

$$(\text{ALE before control}) - (\text{ALE after control}) - (\text{annual cost of control}) = \text{ROSI}$$

For example, the ALE of the threat of an attacker bringing down a Web server is \$12,000, and after the suggested safeguard is implemented, the ALE is valued at \$3,000. The annual cost of maintenance and operation of the safeguard is \$650, so the ROSI is \$8,350 each year as expressed in the following equation:

$$\$12,000 - \$3,000 - \$650 = \$8,350.$$

Results of the Quantitative Risk Analyses

The input items from the quantitative risk analyses provide clearly defined goals and results. The following items generally are derived from the results of the previous steps:

- Assigned monetary values for assets
- A comprehensive list of significant threats
- The probability of each threat occurring
- The loss potential for the company on a per-threat basis over 12 months
- Recommended safeguards, controls, and actions

You have seen for yourself how all of these calculations are based on subjective estimates. Key numbers that provide the basis for the results are not drawn from objective equations or well-defined actuarial datasets but rather from the opinions of those performing the assessment. The AV, SLE, ARO, and cost of controls are all numbers that the participants themselves insert (after much discussion and compromise, typically).

Qualitative Risk Assessment

What differentiates qualitative risk assessment from quantitative risk assessment is that in the former you do not try to assign hard financial values to assets, expected losses, and cost of controls. Instead, you calculate relative values. Risk analysis is usually conducted through a combination of questionnaires and collaborative workshops involving people from a variety of groups within the organization such as information security experts; information technology managers and staff; business asset owners and users; and senior managers. If used, questionnaires are typically distributed a few days to a few weeks ahead of the first workshop. The questionnaires are designed to discover what assets and controls are already deployed, and the information gathered can be very helpful during the workshops that follow. In the workshops participants identify assets and estimate their relative values. Next they try to figure out what threats each asset may be facing, and then they try to imagine what types of vulnerabilities those threats might exploit in the future. The information security experts and the system administrators typically come up with controls to mitigate the risks for the group to consider and the approximate cost of each control. Finally, the results are presented to management for consideration during a cost-benefit analysis.

As you can see, the basic process for qualitative assessments is very similar to what happens in the quantitative approach. The difference is in the details. Comparisons between the value of one asset and another are relative, and participants do not invest a lot of time trying to calculate precise financial numbers for asset valuation. The same is true for calculating the possible impact from a risk being realized and the cost of implementing controls.

The benefits of a qualitative approach are that it overcomes the challenge of calculating accurate figures for asset value, cost of control, and so on, and the process is much less demanding on staff. Qualitative risk management projects can typically start to show significant results within a few weeks, whereas most organizations that choose a quantitative approach see little benefit for months, and sometimes even years, of effort. The drawback of a qualitative approach is that the resulting figures are vague; some Business Decision Makers (BDMs), especially those with finance or accounting backgrounds, may not be comfortable with the relative values determined during a qualitative risk assessment project.

Comparing the Two Approaches

Both qualitative and quantitative approaches to security risk management have their advantages and disadvantages. Certain situations may call for organizations to adopt the quantitative approach. Alternatively, organizations of small size or with limited resources will probably find the qualitative approach much more to their liking. The following table summarizes the benefits and drawbacks of each approach:

Table 2.1: Benefits and Drawbacks of Each Risk Management Approach

	Quantitative	Qualitative
Benefits	• Risks are prioritized by financial impact; assets are prioritized by financial values. • Results facilitate management of risk by return on security investment. • Results can be expressed in management-specific terminology (for example, monetary values and probability expressed as a specific percentage). • Accuracy tends to increase over time as the organization builds historic record of data while gaining experience.	• Enables visibility and understanding of risk ranking. • Easier to reach consensus. • Not necessary to quantify threat frequency. • Not necessary to determine financial values of assets. • Easier to involve people who are not experts on security or computers.
Drawbacks	• Impact values assigned to risks are based on subjective opinions of participants. • Process to reach credible results and consensus is very time consuming. • Calculations can be complex and time consuming. • Results are presented in monetary terms only, and they may be difficult for non-technical people to interpret. • Process requires expertise, so participants cannot be easily coached through it.	• Insufficient differentiation between important risks. • Difficult to justify investing in control implementation because there is no basis for a cost-benefit analysis. • Results are dependent upon the quality of the risk management team that is created.

In years past, the quantitative approaches seemed to dominate security risk management; however, that has changed recently as more and more practitioners have admitted that strictly following quantitative risk management processes typically results in difficult, long-running projects that see few tangible benefits. As you will see in subsequent chapters, the Microsoft security risk management process combines the best of both methodologies into a unique, hybrid approach.

The Microsoft Security Risk Management Process

The Microsoft security risk management process is a hybrid approach that joins the best elements of the two traditional approaches. As you will see in the chapters that follow, this guide presents a unique approach to security risk management that is significantly faster than a traditional quantitative approach. Yet it still provides results that are more detailed and easily justified to executives than a typical qualitative approach. By combining the simplicity and elegance of the qualitative approach with some of the rigor of the quantitative approach, this guide offers a unique process for managing security risks that is both effective and usable. The goal of the process is for stakeholders to be able to understand every step of the assessment. This approach, significantly simpler than traditional quantitative risk management, minimizes resistance to results of the risk analysis and decision support phases, enabling consensus to be achieved more quickly and maintained throughout the process.

The Microsoft security risk management process consists of four phases. The first, the Assessing Risk phase, combines aspects of both quantitative and qualitative risk assessment methodologies. A qualitative approach is used to quickly triage the entire list of security risks. The most serious risks identified during this triage are then examined in more detail using a quantitative approach. The result is a relatively short list of the most important risks that have been examined in detail.

This short list is used during the next phase, Conducting Decision Support, in which potential control solutions are proposed and evaluated and the best ones are then presented to the organization's Security Steering Committee as recommendations for mitigating the top risks. During the third phase, Implementing Controls, the Mitigation Owners actually put control solutions in place. The fourth phase, Measuring Program Effectiveness, is used to verify that the controls are actually providing the expected degree of protection and to watch for changes in the environment such as new business applications or attack tools that might change the organization's risk profile.

Because the Microsoft security risk management process is ongoing, the cycle restarts with each new risk assessment. The frequency with which the cycle recurs will vary from one organization to another; many find that an annual recurrence is sufficient so long as the organization is proactively monitoring for new vulnerabilities, threats, and assets.

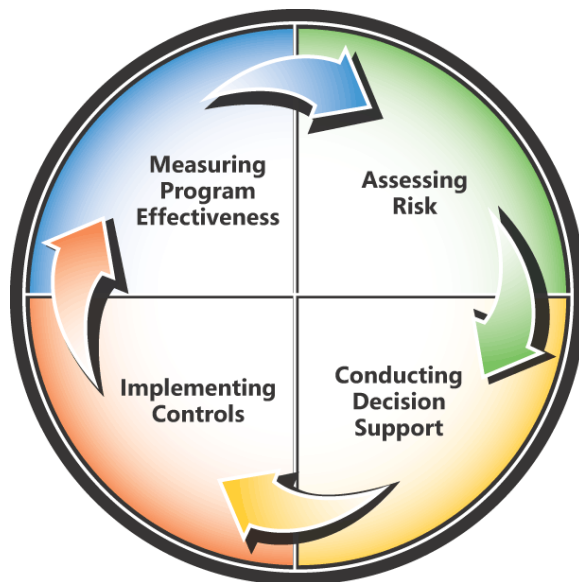


Figure 2.2: Phases of the Microsoft Security Risk Management Process

Figure 2.2 illustrates the four phases of the Microsoft security risk management process. The next chapter, Chapter 3, "Security Risk Management Overview," provides a comprehensive look at the process. The chapters that succeed it explain in detail the steps and tasks associated with each of the four phases.

Chapter 3: Security Risk Management Overview

This chapter is the first in this guide to provide a full summary of the Microsoft security risk management process. After this overview, the chapter discusses several topics that will assist readers as they implement the process. These topics help provide a solid foundation for a successful security risk management program and include:

- Distinguishing risk management from risk assessment.
- Communicating risk effectively.
- Evaluating the maturity of your current risk management practices.
- Defining roles and responsibilities.

It is also important to note that risk management is only one part of a larger governance program for corporate leadership to monitor the business and make informed decisions. While governance programs vary widely, all programs require a structured security risk management component to prioritize and mitigate security risks. The Microsoft security risk management process concepts may be applied to any governance program to help define and manage risks to acceptable levels.

The Four Phases of the Microsoft Security Risk Management Process

Chapter 2, "Survey of Risk Management Practices," introduced the Microsoft security risk management process and defined risk management as an ongoing process with four primary phases:

1. **Assessing Risk.** Identify and prioritize risks to the business.
2. **Conducting Decision Support.** Identify and evaluate control solutions based on a defined cost-benefit analysis process.
3. **Implementing Controls.** Deploy and operate control solutions to reduce risk to the business.
4. **Measuring Program Effectiveness.** Analyze the risk management process for effectiveness and verify that controls are providing the expected degree of protection.

This four-part risk management cycle summarizes the Microsoft security risk management process and is also used to organize content throughout this guide.

Before defining specific practices within the Microsoft security risk management process, however, it is important to understand the larger risk management process and its components. Each phase of the cycle contains multiple, detailed steps. The following list outlines each step to help you understand the importance of each one in the guide as a whole:

- **Assessing Risk phase**
 - *Plan data gathering.* Discuss keys to success and preparation guidance.

- *Gather risk data.* Outline the data collection process and analysis.
- *Prioritize risks.* Outline prescriptive steps to qualify and quantify risks.
- **Conducting Decision Support phase**
 - *Define functional requirements.* Define functional requirements to mitigate risks.
 - *Select possible control solutions.* Outline approach to identify mitigation solutions.
 - *Review solution.* Evaluate proposed controls against functional requirements.
 - *Estimate risk reduction.* Endeavor to understand reduced exposure or probability of risks.
 - *Estimate solution cost.* Evaluate direct and indirect costs associated with mitigation solutions.
 - *Select mitigation strategy.* Complete the cost-benefit analysis to identify the most cost effective mitigation solution.
- **Implementing Controls phase**
 - *Seek holistic approach.* Incorporate people, process, and technology in mitigation solution.
 - *Organize by defense-in-depth.* Organize mitigation solutions across the business.
- **Measuring Program Effectiveness phase**
 - *Develop risk scorecard.* Understand risk posture and progress.
 - *Measure program effectiveness.* Evaluate the risk management program for opportunities to improve.

The following figure illustrates each phase and its associated steps.

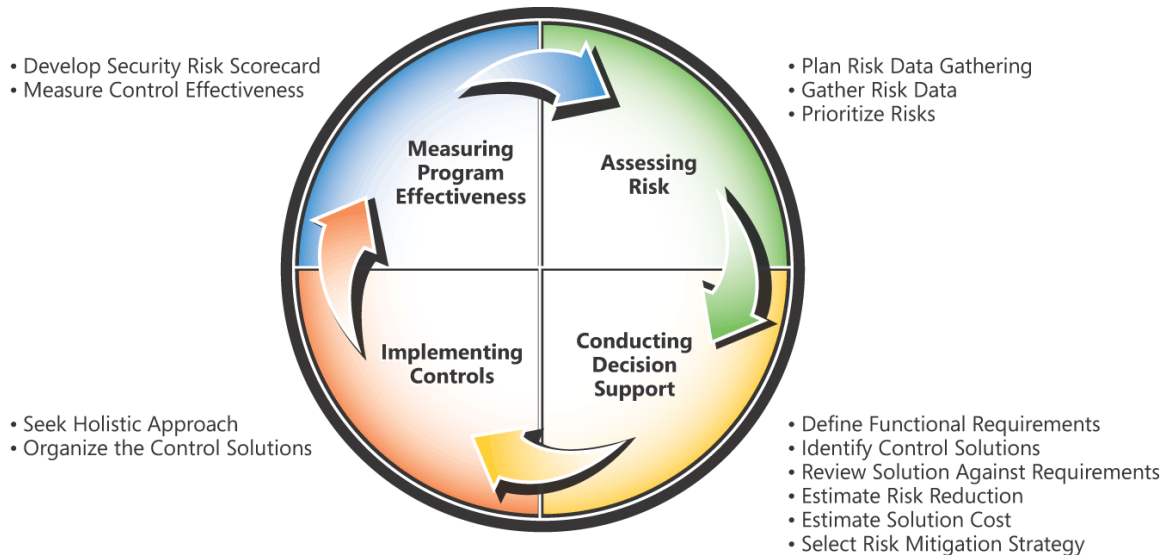


Figure 3.1: The Microsoft Security Risk Management Process

Subsequent chapters in this guide describe, in sequence, each phase in the Microsoft security risk management process. There are several preliminary things to consider, however, before beginning your execution of this process.

Level of Effort

If your organization is relatively new to risk management, it may be helpful to consider which steps in the Microsoft security risk management process typically require the most effort from the Security Risk Management Team. The following figure, based on risk management activities conducted within Microsoft IT, shows relative degrees of effort throughout the process. This perspective may be helpful when describing the overall process and time commitment to organizations that are new to risk management. The relative levels of effort may also be helpful as a guide to avoid spending too much time in one point of the overall process. To summarize the level of effort throughout the process, the figure demonstrates a moderate level of effort to gather data, a lower level for summary analysis, followed by high levels of effort to build detailed lists of risks and conduct the decision support process. For an additional view of tasks and associated effort, refer to the sample project schedule in the Tools folder, SRMGTool4-Sample Project Schedule.xls. The remaining chapters in this guide further describe each step shown below.

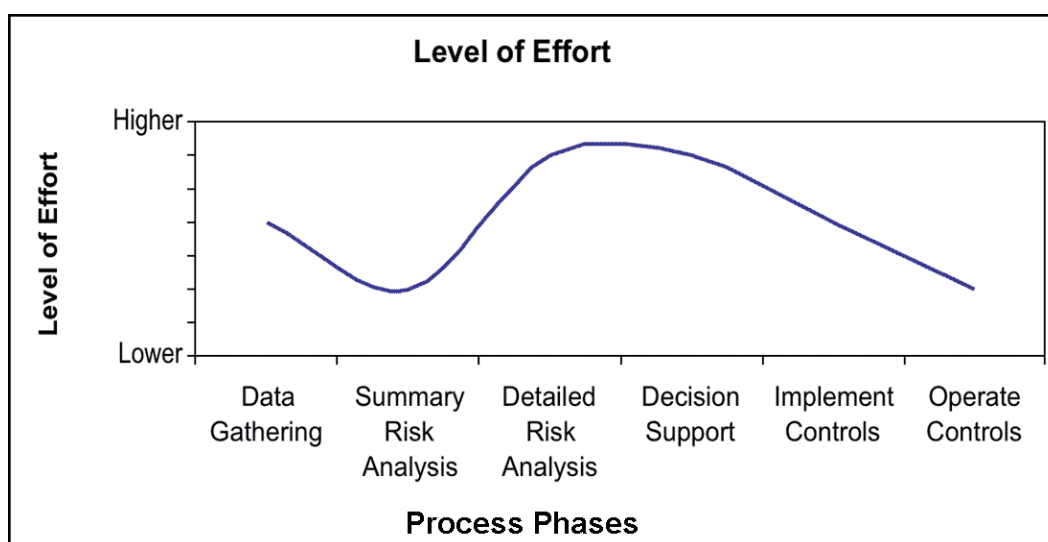


Figure 3.2: Relative Level of Effort During the Microsoft Security Risk Management Process

Laying the Foundation for the Microsoft Security Risk Management Process

Before beginning a security risk management effort, it is important to have a solid understanding of the foundational, prerequisite knowledge and tasks of the Microsoft security risk management process, which include:

- Differentiating between risk management and risk assessment.
- Clearly communicating risk.
- Determining your organization's risk management maturity.
- Defining roles and responsibilities for the process.

Risk Management vs. Risk Assessment

As Chapter 2 discussed, the terms *risk management* and *risk assessment* are not interchangeable. The Microsoft security risk management process defines risk

management as the overall process to manage risk to an acceptable level across the business. Risk assessment is defined as the process to identify and prioritize risks to the business. As outlined in the previous diagram, risk management is comprised of four primary phases: Assessing Risk, Conducting Decision Support, Implementing Controls, and Measuring Program Effectiveness. Risk assessment, in the context of the Microsoft security risk management process, refers only to the Assessing Risk phase within the larger risk management cycle.

Another distinction between risk management and risk assessment is the frequency of initiation of each process. Risk management is defined as an ongoing cycle, but it is typically re-started at regular intervals to refresh the data in each stage of the management process. The risk management process is normally aligned with an organization's fiscal accounting cycle to align budget requests for controls with normal business processes. An annual interval is most common for the risk management process to align new control solutions with annual budgeting cycles.

Although risk assessment is a required, discrete phase of the risk management process, the Information Security Group may conduct multiple risk assessments independent of the current risk management phase or budgeting cycle. The Information Security Group may initiate them anytime a potentially security-related change occurs within the business, such as the introduction of new business practices, or discovered vulnerabilities, changes to the infrastructure. These frequent risk assessments are often referred to as ad-hoc risk assessments, or limited scope risk assessments, and should be viewed as complementary to the formal risk management process. Ad-hoc assessments usually focus on one area of risk within the business and do not require the same amount of resources as the risk management process as a whole. Appendix A, "Ad-Hoc Assessments," outlines and provides an example template of an ad-hoc risk assessment.

Table 3.1: Risk Management vs. Risk Assessment

	Risk Management	Risk Assessment
Goal	Manage risks across business to acceptable level	Identify and prioritize risks
Cycle	Overall program across all four phases	Single phase of risk management program
Schedule	Ongoing	As needed
Alignment	Aligned with budgeting cycles	N/A

Communicating Risk

Various people involved in the risk management process often define the term risk differently. In order to ensure consistency across all stages of the risk management cycle, the Microsoft security risk management process requires that everyone involved understand and agree upon a single definition of the term risk. As defined in Chapter 1, "Introduction to the Security Risk Management Guide," risk is the probability of an impact occurring to the business. This definition requires the inclusion of both an impact statement and a prediction of when the impact may occur, or, in other words, probability of impact. When both elements of risk (probability and impact) are included in a risk statement, the process refers to this as a well-formed risk statement. Use the term to help ensure consistent understanding of the compound nature of risk. The following diagram depicts risk at this most basic level.

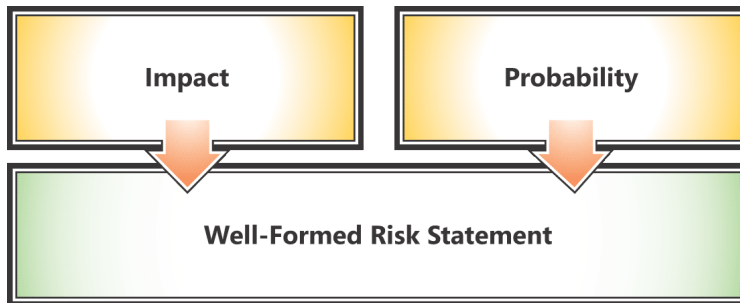


Figure 3.3: Well-Formed Risk Statement

It is important that everyone involved in the risk management process understand the complexity within each element of the risk definition. Only with a thorough understanding of risk will the business be able to take specific action when managing it. For example, defining impact to the business requires information about which asset is affected, what kind of damage may occur, and the extent of damage to the asset. Next, to determine the probability of the impact occurring, you must understand how each impact may occur and how effective the current control environment will be at reducing the probability of the risk.

Using terms defined in Chapter 1, "Introduction to the Security Risk Management Guide," the following risk statement provides guidance in demonstrating both elements of impact and the probability of impact:

Risk is the probability of a vulnerability being exploited in the current environment, leading to a degree of loss of confidentiality, integrity, or availability, of an asset.

The Microsoft security risk management process provides the tools to consistently communicate and measure the probability and degree of loss for each risk. The chapters in this guide walk through the process to establish each component of the well-formed risk statement to identify and prioritize risks across the business. The following diagram builds upon the basic risk statement discussed previously to show the relationships of each element of risk.

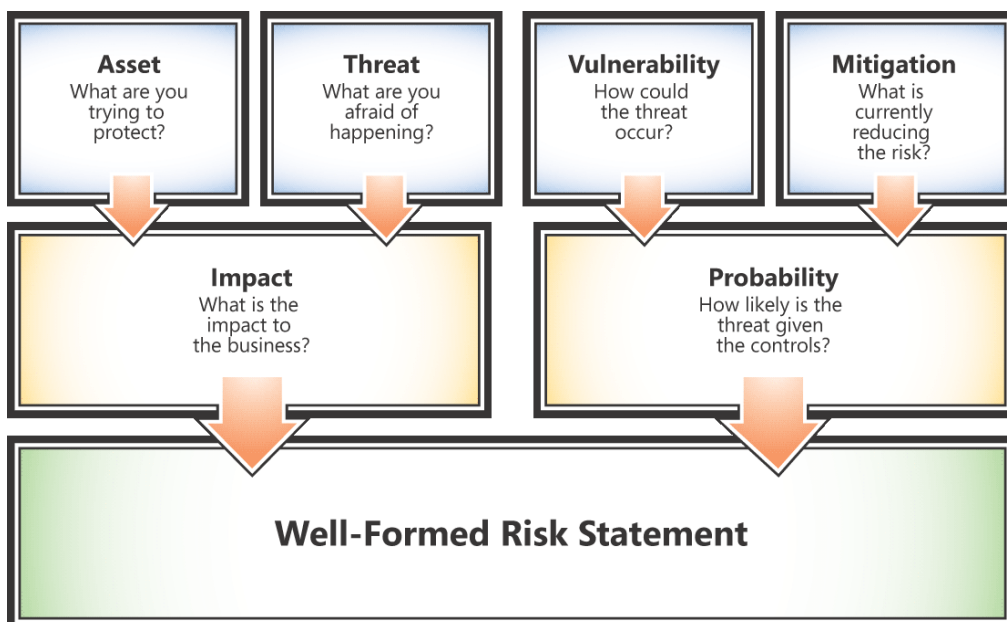


Figure 3.4: Components of the Well-Formed Risk Statement

To help communicate the extent of impact and the degree of probability in the risk statement, the Microsoft security risk management process begins prioritizing risk by using relative terms such as high, moderate, and low. Although this basic terminology simplifies the selection of risk levels, it does not provide sufficient details when you conduct a cost-benefit analysis to select the most efficient mitigation option. To address this weakness of the basic qualitative approach, the process provides tools to generate a detailed level comparison of risks. The process also incorporates quantitative attributes to further aid the cost-benefit analysis for selecting controls.

A common pitfall of risk management disciplines is that they often do not consider the qualitative definitions such as high, moderate, and low risks to the business. Many risks will be identified in your security risk management program. Although the Microsoft security risk management process provides guidance to consistently apply qualitative and quantifiable risk estimates, it is the Security Risk Management Team's responsibility to define the meaning of each value in specific business terms. For example, a high risk to your business may mean a vulnerability occurring within one year, leading to the loss of integrity of your organization's most important intellectual property. The Security Risk Management Team must populate the definitions of each element of the well-formed risk statement. The next chapter provides prescriptive guidance on defining risk levels. It should assist you in defining risk levels for your unique business. The process simply facilitates the exercise, helping to achieve consistency and visibility throughout the process.

Determining Your Organization's Risk Management Maturity Level

Before an organization attempts to implement the Microsoft security risk management process, it is important that it examines its level of maturity with regard to security risk management. An organization that has no formal policies or processes relating to security risk management will find it extremely difficult to put all aspects of the process into practice at once. Even organizations with some formal policies and guidelines that most employees follow fairly well may find the process a bit overwhelming. For these reasons, it is important that you make an estimate of your own organization's maturity level. If you find that your organization is still relatively immature, then you may want to introduce the process in incremental stages over several months, perhaps by piloting it in a single business unit until the cycle has been completed several times. Having demonstrated the effectiveness of the Microsoft security risk management process through this pilot program, the Security Risk Management Team could then slowly introduce it to other business units until the entire organization is using it.

How do you determine the maturity level of your organization? As part of Control Objectives for Information and Related Technology (CobiT), the IT Governance Institute (ITGI) includes an IT Governance Maturity Model. You may want to acquire and review CobiT for a detailed method for determining your organization's level of maturity. The Microsoft security risk management process summarizes elements used in CobiT and presents a simplified approach based on models also developed by Microsoft Services. The maturity level definitions presented here are based on the International Standards Organization (ISO) Information technology—Code of practice for information security management, also known as ISO 17799.

You can estimate your organization's level of maturity by comparing it to the definitions presented in the following table.

Table 3.2: Security Risk Management Maturity Levels

Level	State	Definition
0	Non-Existent	Policy (or process) is not documented, and previously the organization was unaware of the business risk associated with this risk management. Therefore, there has been no communication on the issue.
1	Ad-Hoc	It is clear that some members of the organization have concluded that risk management has value. However, risk management efforts are performed in an ad-hoc manner. There are no documented processes or policies and the process is not fully repeatable. Overall, risk management projects seem chaotic and uncoordinated, and results are not measured and audited.
2	Repeatable	There is awareness of risk management throughout the organization. The risk management process is repeatable yet immature. The process is not fully documented; however, the activities occur on a regular basis, and the organization is working toward establishing a comprehensive risk management process with senior management involvement. There is no formal training or communication on risk management; responsibility for implementation is left to individual employees.
3	Defined Process	The organization has made a formal decision to adopt risk management wholeheartedly in order to drive its information security program. A baseline process has been developed in which there are clearly defined goals with documented processes for achieving and measuring success. Additionally, some rudimentary risk management training is available for all staff. Finally, the organization is actively implementing its documented risk management processes.
4	Managed	There is a thorough understanding of risk management at all levels of the organization. Risk management procedures exist, the process is well defined, awareness is broadly communicated, rigorous training is available, and some initial forms of measurement are in place to determine effectiveness. Sufficient resources have been committed to the risk management program, many parts of the organization are enjoying its benefits, and the Security Risk Management Team is able to continuously improve its processes and tools. There is some use of technological tools to help with risk management, but many if not most risk assessment, control identification, and cost-benefit analysis procedures are manual.
5	Optimized	The organization has committed significant resources to security risk management, and staff members are looking toward the future trying to ascertain what the issues and solutions will be in the months and years ahead. The risk management process is well understood and significantly automated through the use of tools (either developed in-house or acquired from independent software vendors). The root cause of all security issues is identified, and suitable actions are taken to minimize the risk of repetition. Training across a range of levels of expertise is available to staff.

Organizational Risk Management Maturity Level Self Assessment

The following list of assessments offers a more rigorous way to measure your organizational maturity level. The topics elicit subjective responses, but by honestly considering each of them you should be able to determine how well prepared your organization is for implementation of the Microsoft security risk management process. Score your organization on a scale of 0 to 5, using the previous maturity level definitions as a guide.

- Information security policies and procedures are clear, concise, well-documented, and complete.
- All staff positions with job responsibilities involving information security have clearly articulated and well understood roles and responsibilities.
- Policies and procedures for securing third-party access to business data are well-documented. For example, remote vendors performing application development for an internal business tool have sufficient access to network resources to effectively collaborate and complete their work, but they have only the minimum amount of access that they need.
- An inventory of Information Technology (IT) assets such as hardware, software, and data repositories is accurate and up-to-date.
- Suitable controls are in place to protect business data from unauthorized access by both outsiders and insiders.
- Effective user awareness programs such as training and newsletters regarding information security policies and practices are in place.
- Physical access to the computer network and other information technology assets is restricted through the use of effective controls.
- New computer systems are provisioned following organizational security standards in a standardized manner using automated tools such as disk imaging or build scripts.
- An effective patch management system is able to automatically deliver software updates from most vendors to the vast majority of the computer systems in the organization.
- An incident response team has been created and has developed and documented effective processes for dealing with and tracking security incidents. All incidents are investigated until the root cause is identified and any problems are resolved.
- The organization has a comprehensive anti-virus program including multiple layers of defense, user awareness training, and effective processes for responding to virus outbreaks.
- User provisioning processes are well documented and at least partially automated so that new employees, vendors, and partners can be granted an appropriate level of access to the organization's information systems in a timely manner. These processes should also support the timely disabling and deletion of user accounts that are no longer needed.
- Computer and network access is controlled through user authentication and authorization, restrictive access control lists on data, and proactive monitoring for policy violations.
- Application developers are provided with education and possess a clear awareness of security standards for software creation and quality assurance testing of code.
- Business continuity and business continuity programs are clearly defined, well documented, and periodically tested through simulations and drills.

- Programs have commenced and are effective for ensuring that all staff perform their work tasks in a manner compliant with legal requirements.
- Third-party review and audits are used regularly to verify compliance with standard practices for security business assets.

Calculate your organization's score by adding the scores of all of the previous items. Theoretically, scores could range from 0 to 85; however, few organizations will approach either extreme.

A score of 51 or above suggests that the organization is well prepared to introduce and use the Microsoft security risk management process to its fullest extent. A score of 34 to 50 indicates that the organization has taken many significant steps to control security risks and is ready to gradually introduce the process. Organizations in this range should consider rolling out the process to a few business units over a few months before exposing the entire organization to the process. Organizations scoring below 34 should consider starting very slowly with the Microsoft security risk management process by creating the core Security Risk Management Team and applying the process to a single business unit for the first few months. After such organizations demonstrate the value of the process by using it to successfully reduce risks for that business unit, they should expand it to two or three additional business units as feasible. Continue to move slowly, though, because the changes introduced by the process can be significant. You do not want to disrupt the organization to such a degree that you interfere with its ability to effectively achieve its mission. Use your best judgment in this regard—every system that you leave unprotected is a potential security and liability risk, and your own knowledge of your own systems is best. If you think that it is urgent to move quickly and to disregard the suggestion to move slowly, do that.

You should carefully consider which business unit to use for the pilot programs. Questions to consider relate to how important security is to that business unit, where security is defined in terms of the availability, integrity, and confidentiality of information and services. Examples include:

- Is the security risk management maturity level of that business unit above average when compared to the organization?
- Will the owner of the business unit actively support the program?
- Does the business unit have a high level of visibility within the organization?
- Will the value of the Microsoft security risk management process pilot program be effectively communicated to the rest of the organization if successful?

You should consider these same questions when selecting business units for expansion of the program.

Note The (U.S.) National Institute for Standards and Technology (NIST) provides a [Security Self Assessment Guide for Information Technology Systems](http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf) that may be useful to help determine your maturity level; see <http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>.

Defining Roles and Responsibilities

The establishment of clear roles and responsibilities is a critical success factor for any risk management program due to the requirement for cross-group interaction and segregated responsibilities. The following table describes the primary roles and responsibilities used throughout the Microsoft security risk management process.

Table 3.3: Primary Roles and Responsibilities in the Microsoft Security Risk Management Process

Title	Primary Responsibility
Executive Sponsor	Sponsors all activities associated with managing risk to the business, for example, development, funding, authority, and support for the Security Risk Management Team. This role is usually filled by an executive such as the chief security officer or chief information officer. This role also serves as the last escalation point to define acceptable risk to the business.
Business Owner	Is responsible for tangible and intangible assets to the business. Business owners are also accountable for prioritizing business assets and defining levels of impact to assets. Business owners are usually accountable for defining acceptable risk levels; however, the Executive Sponsor owns the final decision incorporating feedback from the Information Security Group.
Information Security Group	Owns the larger risk management process, including the Assessing Risk and Measuring Program Effectiveness phases. Also defines functional security requirements and measures IT controls and the overall effectiveness of the security risk management program.
Information Technology Group	Includes IT architecture, engineering, and operations.
Security Risk Management Team	Responsible for driving the overall risk management program. Also responsible for the Assessing Risk phase and prioritizing risks to the business. At a minimum, the team is comprised of a facilitator and note taker.
Risk Assessment Facilitator	As lead role on the Security Risk Management Team, conducts the data gathering discussions. This role may also lead the entire risk management process.
Risk Assessment Note Taker	Records detailed risk information during the data gathering discussions.
Mitigation Owners	Responsible for implementing and sustaining control solutions to manage risk to an acceptable level. Includes the IT Group and, in some cases, Business Owners.
Security Steering Committee	Comprised of the Security Risk Management Team, representatives from the IT Group, and specific Business Owners. The Executive Sponsor usually chairs this committee. Responsible for selecting mitigation strategies and defining acceptable risk for the business.
Stakeholder	General term referring to direct and indirect participants in a given process or program; used throughout the Microsoft security risk management process. Stakeholders may also include groups outside IT, for example, finance, public relations, and human resources.

The Security Risk Management Team will encounter first-time participants in the risk management process who may not fully understand their roles. Always take the opportunity to provide an overview of the process and its participants. The objective is to build consensus and highlight the fact that every participant has ownership in managing

risk. The following diagram, which summarizes key participants and shows their high-level relationships, can be helpful in communicating the previously-defined roles and responsibilities and should provide an overview of the risk management program.

To summarize, the Executive Sponsor is ultimately accountable for defining acceptable risk and provides guidance to the Security Risk Management Team in terms of ranking risks to the business. The Security Risk Management Team is responsible for assessing risk and defining functional requirements to mitigate risk to an acceptable level. The Security Risk Management Team then collaborates with the IT groups who own mitigation selection, implementation, and operations. The final relationship defined below is the Security Risk Management Team's oversight of measuring control effectiveness. This usually occurs in the form of audit reports, which are also communicated to the Executive Sponsor.

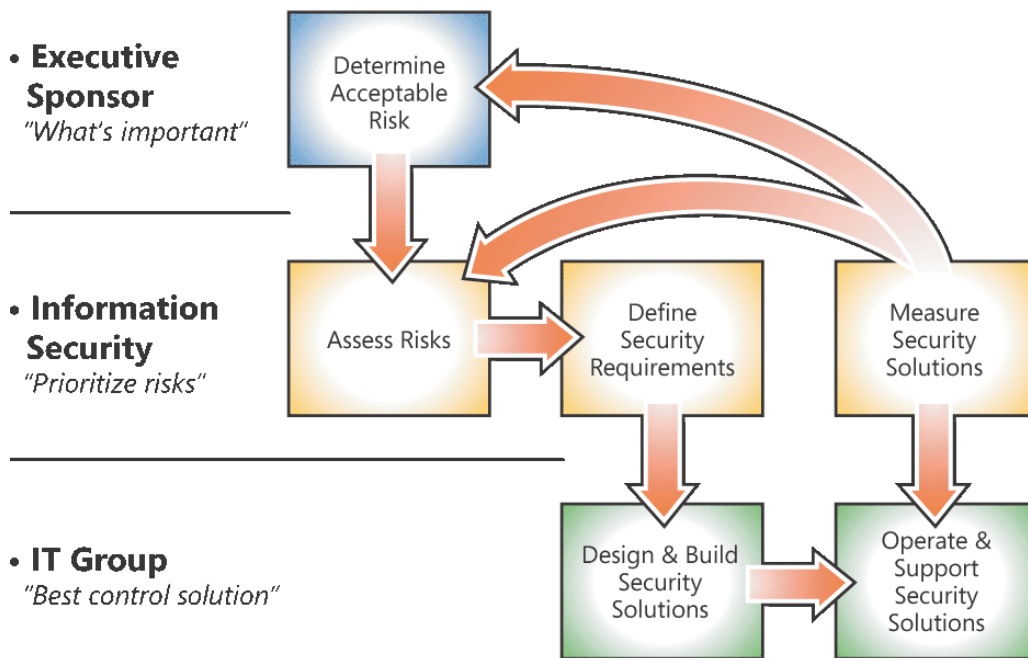


Figure 3.5: Overview of Roles and Responsibilities Used Throughout the Microsoft Security Risk Management Process

Building the Security Risk Management Team

Before starting the risk assessment process, do not overlook the need to clearly define roles within the Security Risk Management Team. Because the risk management scope includes the entire business, non-Information Security Group members may request to be part of the team. If this occurs, outline clear roles for each member and align with the roles and responsibilities defined in the overall risk management program above. Investing in role definition early reduces confusion and assists decision making throughout the process. All members on the team must understand that the Information Security Group owns the overall process. Ownership is important to define because Information Security is the only group that is a key stakeholder in every stage of the process, including executive reporting.

Security Risk Management Team Roles and Responsibilities

After assembling the Security Risk Management Team, it is important to create specific roles and to maintain them throughout the entire process. The primary roles of the Risk Assessment Facilitator and the Risk Assessment Note Taker are described below.

The Risk Assessment Facilitator must have extensive knowledge of the entire risk management process and a thorough understanding of the business, as well as an understanding of the technical security risks that underlie the business functions. He or she must be able to translate business scenarios into technical risks while conducting the risk discussions. As an example, the Risk Assessment Facilitator needs to understand both the technical threats to and vulnerabilities of mobile workers and the business value of such workers. For example, customer payments will not be processed if a mobile worker cannot access the corporate network. The Risk Assessment Facilitator must understand scenarios such as these and be able to identify the technical risks and potential control requirements, such as mobile device configuration and authentication requirements. If possible, select a Risk Assessment Facilitator who has performed risk assessments in the past and who understands the overall priorities of the business.

If a facilitator with risk assessment experience is unavailable, enlist the assistance of a qualified partner or consultant. However, be sure to include an Information Security Group member who understands the business and the stakeholders involved.

Note Outsourcing the risk assessment facilitation role may be attractive, but beware of losing the stakeholder relationship, business, and security knowledge when the consultants leave. Do not underestimate the value that a risk management process brings to the stakeholders as well as the Information Security Group.

The Risk Assessment Note Taker is responsible for capturing notes and documenting the planning and data gathering activities. This responsibility may seem too informal for role definition at this stage; however, solid note taking skills pay off in the prioritization and decision support processes later in the process. One of the most important aspects of managing risk is communicating risk in terms that stakeholders understand and can apply to their business. A thorough note taker makes this process easier by providing written documentation when needed.

Summary

Chapters 1-3 provide an overview of risk management and define the goals and approach to begin building the foundation for a successful implementation of the Microsoft security risk management process. The next chapter covers the first phase, Assessing Risk, in detail. Subsequent chapters follow each phase of the risk management process, Conducting Decision Support, Implementing Controls, and Measuring Program Effectiveness.

Chapter 4: Assessing Risk

Overview

The overall risk management process comprises four primary phases: Assessing Risk, Conducting Decision Support, Implementing Controls, and Measuring Program Effectiveness. The risk management process illustrates how a formal program provides a consistent path for organizing limited resources to manage risk across an organization. The benefits are realized by developing a cost-effective control environment that drives and measures risk to an acceptable level.

The Assessing Risk phase represents a formal process to identify and prioritize risks across the organization. The Microsoft security risk management process provides detailed direction on performing risk assessments and breaks down the process in the Assessing Risk phase into the following three steps:

1. **Planning.** Building the foundation for a successful risk assessment.
2. **Facilitated data gathering.** Collecting risk information through facilitated risk discussions.
3. **Risk prioritization.** Ranking identified risks in a consistent and repeatable process.

The output of the Assessing Risk phase is a prioritized list of risks that provide the inputs to the Conducting Decision Support phase, which Chapter 5, "Conducting Decision Support," addresses in detail.

The following diagram provides a review of the overall risk management process and demonstrates the role of risk assessment in the larger program. The three steps within the Assessing Risk phase are also highlighted.

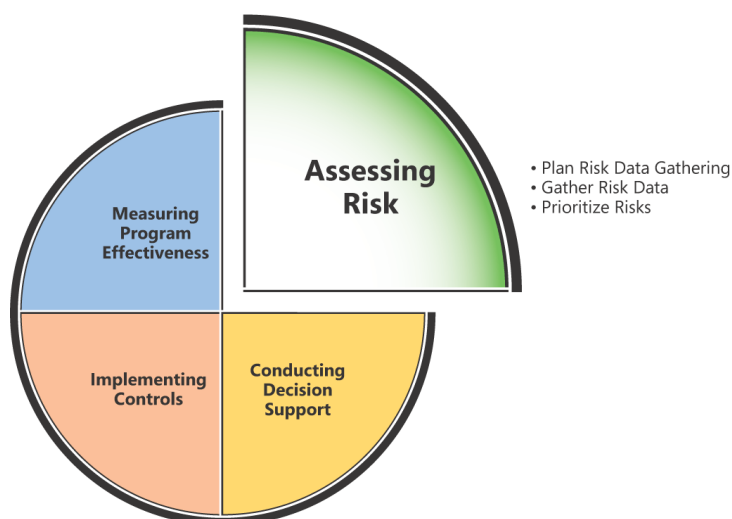


Figure 4.1: The Microsoft Security Risk Management Process: Assessing Risk Phase

Planning

Proper risk assessment planning is critical to the success of the entire risk management program. Failure to adequately align, scope, and gain acceptance of the Assessing Risk phase diminishes the effectiveness of the other phases in the larger program. Conducting risk assessments can be a complicated process that requires significant investment to complete. Tasks and guidance critical to the planning step are covered in the next section of this chapter.

Facilitated Data Gathering

After planning, the next step is to gather risk related information from stakeholders across the organization; you will also use this information in the Conducting Decision Support phase. The primary data elements collected during the facilitated data gathering step are:

- **Organizational assets.** Anything of value to the business.
- **Asset description.** Brief explanation of each asset, its worth, and ownership to facilitate common understanding throughout the Assessing Risk phase.
- **Security threats.** Causes or events that may negatively impact an asset, represented by loss of confidentiality, integrity, or availability of the asset.
- **Vulnerabilities.** Weaknesses or lack of controls that may be exploited to impact an asset.
- **Current control environment.** Description of current controls and their effectiveness across the organization.
- **Proposed controls.** Initial ideas to reduce risk.

The facilitated data gathering step represents the bulk of the cross-group collaboration and interaction during the Assessing Risk phase. The third section in this chapter covers data gathering tasks and guidance in detail.

Risk Prioritization

During the facilitated data gathering step, the Security Risk Management Team begins sorting the large amount of information collected to prioritize risks. The risk prioritization step is the first one within the phase that involves an element of subjectivity. Prioritization is subjective in nature because, after all, the process essentially involves predicting the future. Because the Assessing Risk output drives future Information Technology (IT) investments, establishing a transparent process with defined roles and responsibilities is critical to gain acceptance of the results and motivate action to mitigate risks. The Microsoft security risk management process provides guidance to identify and prioritize risks in a consistent and repeatable way. An open and reproducible approach helps the Security Risk Management Team to reach consensus quickly, minimizing potential delays caused by the subjective nature of risk prioritization. The fourth section in this chapter covers prioritization tasks and guidance in detail.

Required Inputs for the Assessing Risk Phase

Each step in the Assessing Risk phase contains a specific list of prescriptive tasks and associated inputs. The phase itself requires a well-built foundation as opposed to specific inputs. As outlined in Chapter 1, the Assessing Risk phase requires security leadership in the form of executive support, stakeholder acceptance, and defined roles and responsibilities. The following sections address these areas in detail.

Participants in the Assessing Risk Phase

Assessing risk requires cross-group interaction and for different stakeholders to be held responsible for tasks throughout the process. A best practice to reduce role confusion throughout the process is to communicate the checks and balances built into the risk management roles and responsibilities. While you are conducting the assessment, communicate the roles that stakeholders play and assure them the Security Risk Management Team respects these boundaries. The following table summarizes the roles and primary responsibilities for stakeholders in this phase of the risk management process.

Table 4.1: Roles and Responsibilities in the Risk Management Program

Role	Responsibility
Business Owner	Determines value of business assets
Information Security Group	Determines probability of impact on business assets
Information Technology: Engineering	Designs technical solutions and estimates engineering costs
Information Technology: Operations	Designs operational components of solution and estimates operating costs

The built-in tactical checks and balances will become apparent during the following sections that closely examine the planning, facilitated data gathering, and risk prioritization steps of the Assessing Risk phase.

Tools Provided for the Assessing Risk Phase

During this risk assessment process you will gather data about risks and then use this data to prioritize the risks. Four tools are included to assist in this phase. You can find the tools in the Tools and Templates folder that was created when you unpacked the archive containing this guide and its related files.

- **Data gathering template** (SRMGTool1-Data Gathering Tool.doc). A template to assist in facilitating discussions to gather risk data.
- **Summary Level Risk Analysis Worksheet** (SRMGTool2-Summary Risk Level.xls). This Microsoft® Excel worksheet will help your organization to conduct the first pass of risk analysis: the summary level analysis.
- **Detail Level Risk Analysis Worksheet** (SRMGTool3-Detailed Level Risk Prioritization.xls). This Excel worksheet will help your organization to conduct a more exhaustive analysis of the top risks identified during the summary level analysis.
- **Sample schedule** (SRMGTool4-Sample Project Schedule.xls). This schedule may assist you in planning activities for this phase.

There is also a useful resource for this chapter in Appendix B: Common Information Systems Assets which lists information system assets typically found in organizations of various types.

Required Output for the Assessing Risk Phase

The output of the Assessing Risk phase is a prioritized list of risks, including qualitative ranking and quantitative estimates used in the Conducting Decision Support phase that the next chapter describes.

Planning

The planning step is arguably the most important to ensure stakeholder acceptance and support throughout the risk assessment process. Stakeholder acceptance is critical, because the Security Risk Management Team requires active participation from other stakeholders. Support is also critical because the assessment results may influence stakeholder budgeting activities if new controls are required to reduce risk. The primary tasks in the planning step are to properly align the Assessing Risk phase to business processes, accurately scope the assessment, and gain stakeholder acceptance. The following section examines these three tasks in more detail and covers success factors related to those tasks.

Alignment

It is ideal to begin the Assessing Risk phase prior to your organization's budgeting process. Alignment facilitates executive support and increases visibility within the organization and IT groups while they develop budgets for the next fiscal year. Proper timing also aids in building consensus during the assessment because it allows stakeholders to take active roles in the planning process. The Information Security Group is often viewed as a reactive team that disrupts organization activity and surprises business units with news of control failures or work stoppages. Sensible timing of the assessment is critical to build support and helping the organization understand that security is everyone's responsibility and is engrained in the organization. Another benefit of conducting a risk assessment is demonstrating that the Information Security Group can be viewed as a proactive partner rather than a simple policy enforcer during emergencies. This guide provides a sample project timeline to aid in aligning the risk assessment process to your organization. Obviously, the Security Risk Management Team should not withhold risk information while waiting for the budgeting cycle. Alignment of the timing of the assessment is simply a best practice learned from conducting assessments in Microsoft IT.

Note Proper alignment of the risk management process with the budget planning cycle may also benefit internal or external auditing activities; however, coordinating and scoping audit activities are outside the scope of this guide.

Scoping

During planning activities, clearly articulate the scope of the risk assessment. To effectively manage risk across the organization, the risk assessment scope should document all organization functions included in the risk assessment. If your organization's size does not allow an enterprise wide risk assessment, clearly articulate which part of the organization will be in scope, and define the associated stakeholders. As discussed in Chapter 2, if your organization is new to risk management programs, you may want to start with well-understood business units to practice the risk assessment process. For example, selecting a specific human resources application or IT service, such as remote access, may help demonstrate the value of the process and assist in building momentum for an organization-wide risk assessment.

Note Organizations often fail to accurately scope a risk assessment. Clearly define the areas of the organization to be evaluated and gain executive approval before moving forward. The scope should be discussed often and understood at all stakeholder meetings throughout the process.

In the planning step you must also define the scope of the risk assessment itself. The information security industry uses the term assessment in many ways that may confuse non-technical stakeholders. For example, vulnerability assessments are performed to identify technology-specific configuration or operational weaknesses. The term compliance assessment may be used to communicate an audit, or measurement of current controls against formal policy. The Microsoft security risk management process defines risk assessment as *the process to identify and prioritize enterprise IT security risks to the organization*. You may adjust this definition as appropriate for your organization. For example, some Security Risk Management Teams may also include personnel security in the scope of their risk assessments.

Stakeholder Acceptance

Risk assessment requires active stakeholder participation. As a best practice, work with stakeholders informally and early in the process to ensure that they understand the importance of the assessment, their roles, and the time commitment asked of them. Any experienced Risk assessment Facilitator can tell you that there is a difference between stakeholder approval of the project versus stakeholder acceptance of the time and priority of the project. A best practice to enlist stakeholder support is to pre-sell the concept and the activities within the risk assessment. Pre-selling may involve an informal meeting with stakeholders before a formal commitment is requested. Emphasize why a proactive assessment helps the stakeholder in the long run by identifying controls that may avoid disruptions from security events in the future. Including past security incidents as examples in the discussion is an effective way to remind stakeholders of potential organization impacts.

Note To help stakeholders understand the process, prepare a short summary communicating the justification and value of the assessment. Share the summary as much as possible. You will know that you have been effective when you hear stakeholders describing the assessment to each other. This guide's executive summary provides a good starting point to communicate the value of the risk assessment process.

Preparing for Success: Setting Expectations

Proper expectation setting cannot be overemphasized. Setting reasonable expectations is critical if the risk assessment is to be successful, because the process requires significant contributions from different groups that possibly represent the entire organization. Furthermore, participants need to agree and understand success factors for their role and the larger process. If even one of these groups does not understand or actively participate, the effectiveness of the entire program may be compromised.

While you build consensus during the planning step, set expectations up front on the roles, responsibilities, and participation levels asked of other stakeholders. You also should share the challenges that the assessment presents. For example, clearly describe the processes of risk identification and prioritization to avoid potential misunderstandings.

Embracing Subjectivity

Business Owners are sometimes nervous when an outside group (in this case, the Information Security Group) predicts possible security risks that may impact fiscal priorities. You can reduce this natural tension by setting expectations about the goals of the risk assessment process and to assure stakeholders that roles and responsibilities will be respected throughout the process. Specifically, the Information Security Group

must recognize that Business Owners define the value of business assets. This also means that stakeholders must rely on the Information Security Group's expertise to estimate the probability of threats impacting the organization. Predicting the future is subjective in nature. Business Owners must acknowledge and support the fact that the Information Security Group will use its expertise to estimate probabilities of risks. Call out these relationships early and showcase the credentials, experience, and shared goals of the Information Security Group and Business Owners.

After completing the planning step, articulating roles and responsibilities, and properly setting expectations, you are ready to begin the field work steps of the risk assessment process: facilitated data gathering and risk prioritization. The next two sections detail these steps before moving on in Chapter 5 to discuss the Conducting Decision Support phase.

Facilitated Data Gathering

The overview section of this chapter provides an introduction to the risk assessment process, covering the three primary steps: planning, facilitated data gathering, and risk prioritization. After you complete the planning activities, next you will gather risk data from stakeholders across the organization. You use this information to help identify and ultimately prioritize risks.

This section is organized into three parts. The first describes the data gathering process in detail and focuses on success factors when gathering risk information. The second part explains the detailed steps of gathering risk data through facilitated meetings with technical and non-technical stakeholders. The third part describes the steps to consolidate this compilation of data into a collection of impact statements as described in Chapter 3. To conclude the risk assessment process, this list of impact statements provides the inputs into the prioritization process detailed in the following section.

Data Gathering Keys to Success

You may question the benefit of asking people with no professional experience in security detailed questions about risks related to information technology. Experience conducting risk assessments in Microsoft IT shows that there is tremendous value in asking both technical and non-technical stakeholders for their thoughts regarding risks to organizational assets that they manage. Information security professionals must also gain detailed knowledge of stakeholder concerns to translate information about their environments into prioritized risks. Meeting collaboratively with stakeholders helps them to understand risk in terms that they can comprehend and value. Furthermore, stakeholders either control or influence IT spending. If they do not understand the potential impacts to the organization, the process of allocating resources is much more difficult. Business Owners also drive company culture and influence user behavior. This alone can be a powerful tool when managing risk.

When risks are discovered, the Information Security Group requires stakeholder support in terms of allocating resources and building consensus around risk definition and prioritization. Some Information Security Groups without a proactive risk management program may rely on fear to motivate the organization. This is a short term strategy at best. The Information Security Group must learn to seek the support of the organization if the risk management program is to be sustained over time. The first step to build this support is meeting face-to-face with stakeholders.

Building Support

Business Owners have explicit roles in the risk assessment process. They are responsible for identifying their organizational assets and estimating the costs of potential impacts to those assets. By formalizing this responsibility, the Information Security Group and Business Owners share equally in the success of managing risk. Most information security professionals and non-technical stakeholders do not realize this connection automatically. As the risk management experts, information security professionals must take the initiative to bridge knowledge gaps during risk discussions. As mentioned in the previous chapter, enlisting an executive sponsor who understands the organization makes building this relationship much easier.

Discussing vs. Interrogating

Many security risk management methods require the Information Security Group to ask stakeholders explicit questions and catalog their responses. Examples of this type of questioning are, "Can you please describe your policies to ensure proper segmentation of duties?" and "What is your process for reviewing policies and procedures?" Be aware of the tone and direction of the meeting. A good rule to remember is to focus on open ended questions to help facilitate two way discussions. This also allows stakeholders to communicate the true spirit of answers versus simply telling the Risk Assessment Facilitator what they think he or she wants to hear. The intent of the risk discussion is to understand the organization and its surrounding security risks; it is not to conduct an audit of documented policy. Although non-technical stakeholder input is valuable, it is usually not comprehensive. The Security Risk Management Team—independent of the Business Owner—still needs to research, investigate, and consider all risks for each asset.

Building Goodwill

Information security is a difficult business function because the exercise of reducing risk is often viewed as reducing usability or employee productivity. Use the facilitated discussions as a tool to build an alliance with stakeholders. Legislation, privacy concerns, pressure from competitors, and increased consumer awareness have led executives and Business Decision Makers (BDMs) to recognize that security is a highly important business component. Help stakeholders understand the importance of managing risk and their roles within the larger program. Sometimes relationship building between the Information Security Group and stakeholders is more productive than the actual data collected during the meeting. This is still a small but important victory in the larger risk management effort.

Risk Discussion Preparation

Before the risk discussions commence, the Security Risk Management Team should invest time in researching and clearly understanding each element to be discussed. The following information covers best practices and further defines each element in the well-formed risk statement in preparation for facilitating discussions with stakeholders.

Identifying Risk Assessment Inputs

The risk assessment team must prepare thoroughly before it meets with stakeholders. The team is more effective and discussions are more productive when the team has a clear understanding of the organization, its technical environment, and past assessment activity. Use the following list to help collect material to be used as inputs into the risk assessment process:

- **New business drivers.** Refresh your understanding of the organization priorities or any changes that have occurred since the last assessment. Pay particular attention to any mergers and acquisitions activity.
- **Previous risk assessments.** Review past assessments, which provide perspective. The risk assessment team may have to reconcile the new assessment against previous work.
- **Audits.** Collect any audit reports relevant to the risk assessment scope. Audit results must be accounted for in the assessment and when selecting new control solutions.
- **Security incidents.** Use past incidents to identify key assets, understand the value of assets, identify prevalent vulnerabilities, and highlight control deficiencies.
- **Industry events.** Identify new trends in the organization and external influences. Government regulation, laws, and international activity may significantly affect your risk posture. Identifying new trends may require substantial research and assessment from your organization. It may be helpful to dedicate personnel to review throughout the year.
- **Bulletins.** Review known security issues that are identified on the Web, in newsgroups, and directly from software vendors.
- **Information security guidance.** Conduct research to determine whether new trends, tools, or approaches to risk management are available. Industry standards can be leveraged to improve or help justify the risk assessment process or help identify new control strategies. International standards are another key input.

This guide incorporates concepts from many standards such as the International Standards Organization (ISO) 17799. Careful evaluation and application of standards allows you to use the work of other professionals and provide a degree of credibility with organization stakeholders. It may be helpful to specifically reference standards during risk discussions to ensure the assessment covers all applicable areas of information security.

Identifying and Classifying Assets

The scope of the risk assessment defines the areas of the organization under review in the data gathering discussions. Business assets within this scope must be identified to drive the risk discussions. Assets are defined as anything of value to the organization. This includes intangible assets such as company reputation and digital information and tangible assets such as physical infrastructure. The most effective approach is to be as specific as possible when defining business assets, for example, account information in a customer management application. You should not discuss impact statements when you are defining assets. Impact statements define the potential loss or damage to the organization. One example of an impact statement might be the availability of account data in the customer management application. Impact statements are expanded on later in the risk discussion. Note that each asset may have multiple impacts identified during the discussion.

While you identify assets, also identify or confirm the owner of the asset. It is often more difficult to identify the person or group accountable for an asset than it may seem. Document specific asset owners during the facilitated risk discussions. This information may be useful during the prioritization process in order to confirm information and communicate risks directly to asset owners.

To help categorize assets, it may be helpful to group them into business scenarios, for example, online banking transactions or source code development. When working with non-technical stakeholders, begin the asset discussion with business scenarios. Then document specific assets within each scenario.

After assets have been identified, the second responsibility of the Business Owner is to classify each asset in terms of potential impact to the organization. Classifying assets is a critical component in the overall risk equation. The section below aids in this process.

Assets

Business assets can be tangible or intangible. You must define either type of asset sufficiently enough to allow Business Owners to articulate asset value in terms of the organization. Both categories of assets require the stakeholder to provide estimates in the form of direct monetary loss and indirect financial impact.

Tangible assets include physical infrastructure, such as data centers, servers, and property. Intangible assets include data or other digital information of value to the organization, for example, banking transactions, interest calculations, and product development plans and specifications.

As appropriate for your organization, a third asset definition of IT service may be helpful. IT service is a combination of tangible and intangible assets. For example, a corporate IT e-mail service contains physical servers and uses the physical network; however, the service may contain sensitive digital data. You should also include IT service as an asset because it generally has different owners for data and physical assets. For example, the e-mail service owner is responsible for the availability of accessing and sending e-mail. However, the e-mail service may not be responsible for the confidentiality of financial data within e-mail or the physical controls surrounding e-mail servers. Additional examples of IT services include file sharing, storage, networking, remote access, and telephony.

Asset Classes

Assets within the scope of the assessment must be assigned to a qualitative group, or class. Classes facilitate the definition of the overall impact of security risks. They also help the organization focus on the most critical assets first. Different risk assessment models define a variety of asset classes. The Microsoft security risk management process uses three asset classes to help measure the value of the asset to an organization. Why only three classes? These three groupings allow for sufficient distinction and reduce the time to debate and select the appropriate class designation.

The Microsoft security risk management process defines the following three qualitative asset classes: high business impact (HBI), moderate business impact (MBI), and low business impact (LBI). During the risk prioritization step, the process also provides guidance to quantify assets. As appropriate for your organization, you may choose to quantify assets during the facilitated risk discussions. If you do, beware of the time required to reach consensus on quantifying monetary values during the risk discussion. The process recommends waiting until all risks have been identified and then prioritized to reduce the number of risks needing further analysis.

Note For additional information on defining and categorizing information and information systems, refer to National Institute of Standards and Technology (NIST) Special Publication 800-60 workshops, "Mapping Types of Information and Information Systems to Security Categories," and the Federal Information Processing Standards (FIPS) publication 199, "Security Categorization of Federal Information and Information Systems."

High Business Impact

Impact on the confidentiality, integrity, or availability of these assets causes severe or catastrophic loss to the organization. Impact may be expressed in raw financial terms or may reflect indirect loss or theft of financial instruments, organization productivity, damage to reputation, or significant legal and regulatory liability. The following list offers a few examples within the HBI class:

- **Authentication credentials.** Such as passwords, private cryptographic keys, and hardware tokens.
- **Highly sensitive business material.** Such as financial data and intellectual property.
- **Assets subjected to specific regulatory requirements.** Such as GLBA, HIPAA, CA SB1386, and EU Data Protection Directive.
- **Personally identifiable information (PII).** Any information that would allow an attacker to identify your customers or employees or know any of their personal characteristics.
- **Financial transaction authorization data.** Such as credit card numbers and expiration dates.
- **Financial profiles.** Such as consumer credit reports or personal income statements.
- **Medical profiles.** Such as medical record numbers or biometric identifiers.

To protect the confidentiality of assets in this class, access is intended strictly for limited organizational use on a need-to-know basis. The number of people with access to this data should be explicitly managed by the asset owner. Equitable consideration should be given to the integrity and availability of assets in this class.

Moderate Business Impact

Impact on the confidentiality, integrity, or availability of these assets causes moderate loss to the organization. Moderate loss does not constitute a severe or catastrophic impact but does disrupt normal organizational functions to the degree that proactive controls are necessary to minimize impact within this asset class.

Moderate loss may be expressed in raw financial terms or include indirect loss or theft of financial instruments, business productivity, damage to reputation, or significant legal and regulatory liability. These assets are intended for use for specified groups of employees and/or approved non-employees with a legitimate business need. The following represent examples within the MBI class:

- **Internal business information.** Employee directory, purchase order data, network infrastructure designs, information on internal Web sites, and data on internal file shares for internal business use only.

Low Business Impact

Assets not falling into either the HBI or MBI are classified as LBI and have no formal protection requirements or additional controls beyond standard best practices for securing infrastructure. These assets are typically intended to be widely published information where unauthorized disclosure would not result in any significant financial loss, legal or regulatory problems, operational disruptions, or competitive business disadvantage.

Some examples of LBI assets include but are not limited to:

- High-level organization structure.
- Basic information about the IT operating platform.
- Read access to publicly accessible Web pages.
- Public cryptographic keys.
- Published press releases, product brochures, white papers, and documents included with released products.
- Obsolete business information or tangible assets.

Organizing Risk Information

Risk involves many components across assets, threats, vulnerabilities, and controls. The Risk Assessment Facilitator must be able to determine which risk component is being discussed without interfering with the flow of the conversation. To help organize the discussion, use the risk discussion template (SRMGTool1-Data Gathering Tool.doc) included in the Tools section to help attendees understand the components within risk. The template also assists the Risk Assessment Note Taker in capturing risk information consistently across meetings.

The template can be populated in any sequence. However, experience shows that observing sequence in terms of the following questions helps discussion participants understand the components of risk and uncover more information:

- What asset are you protecting?
- How valuable is the asset to the organization?
- What are you trying to avoid happening to the asset (both known threats and potential threats)?
- How might loss or exposures occur?
- What is the extent of potential exposure to the asset?
- What are you doing today to reduce the probability or the extent of damage to the asset?
- What are some actions that we can take to reduce the probability in the future?

To the information security professional, the previous questions translate into specific risk assessment terminology and categories used to prioritize risk. However, the stakeholder may not be fluent with such terms and is not responsible for prioritizing risk. Experience shows that avoiding information security terminology such as threats, vulnerabilities, and countermeasures improves the quality of discussion and helps non-technical participants not to feel intimidated. Another benefit of using functional terms to discuss risk is to reduce the possibility of other technologists debating subtleties of specific terms. At this point in the process, it is much more important to understand the larger risk areas than to debate competing definitions of threat and vulnerability. The Risk Assessment Facilitator should wait until the end of the discussion to resolve questions around risk definitions and terminology.

Organizing by Defense-in-Depth Layers

The Risk Assessment Note Taker and Facilitator will collect large amounts of information. Use the defense-in-depth model to help organize discussions pertaining to all elements of risk. This organization helps provide structure and assists the Security Risk Management Team in gathering risk information across the organization. An example of defense-in-depth layers is included in the risk discussion template and illustrated in Figure 4.2 below. The section titled "Organizing Control Solutions" in Chapter 6, "Implementing Controls and Measuring Program Effectiveness," includes a more detailed description of the defense-in-depth model.

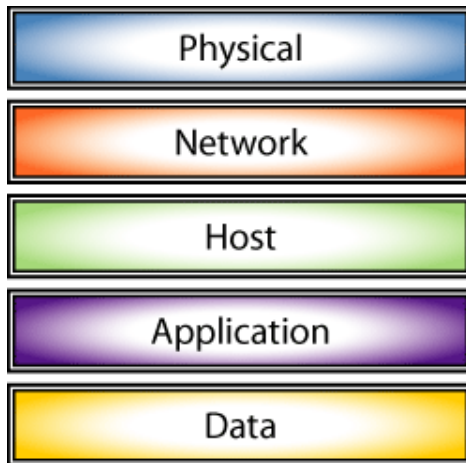


Figure 4.2: Defense-in-Depth Model

Another useful tool to complement the defense-in-depth model is to reference the ISO 17799 standard to organize risk related questions and answers. Referencing a comprehensive standard like ISO 17799 also helps facilitate risk discussions surrounding additional areas, for example, legal, policy, process, personnel, and application development.

Defining Threats and Vulnerabilities

Information on threats and vulnerabilities provides the technical evidence used to prioritize risks across an enterprise. Because many non-technical stakeholders may not be familiar with the detailed exposures affecting their business, the Risk Assessment Facilitator may need to provide examples to help start the discussion. This is one area in which prior research is valuable in terms of helping Business Owners discover and understand risk in their own environments. For reference, ISO 17799 defines threats as a cause of potential impact to the organization. NIST defines a threat as an event or entity with potential to harm the system. Impact resulting from a threat is commonly defined through concepts such as confidentiality, integrity, and availability. Referencing industry standards is especially useful when researching threats and vulnerabilities.

For purposes of the facilitated risk discussion it may be helpful to translate threats and vulnerabilities into familiar terms for non-technical stakeholders. For example, what are you trying to avoid, or what are you afraid will happen to the asset? Most impacts to business can be categorized in terms of confidentiality of the asset, integrity, or availability of the asset to conduct business. Try using this approach if stakeholders are having difficulty understanding the meaning of threats to organizational assets. A common example of a threat to the organization is a breach in the integrity of financial data. After you have articulated what you are trying to avoid, the next task is to determine how threats may occur in your organization.

A vulnerability is a weakness of an asset or group of assets that a threat may exploit. In simplified terms, vulnerabilities provide the mechanism or the how threats may occur. For additional reference, NIST defines vulnerability as a condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat. As an example, a common vulnerability for hosts is the absence of security updates. Incorporating the threat and vulnerability examples previously given produces the following statement: "Unpatched hosts may lead to a breach of the integrity of financial information residing on those hosts."

A common pitfall in performing a risk assessment is a focus on technology vulnerabilities. Experience shows that the most significant vulnerabilities often occur due to lack of

defined process or inadequate accountability for information security. Do not overlook the organizational and leadership aspects of security during the data gathering process. For example, expanding on the security update vulnerability above, the inability to enforce updates on managed systems may lead to a breach of the integrity of financial information residing on those systems. Clear accountability and enforcement of information security policies is often an organizational issue in many businesses.

Note Throughout the data gathering process, you may recognize common groups of threats and vulnerabilities. Keep track of these groups to determine whether similar controls may reduce the probability of multiple risks.

Estimating Asset Exposure

After the Risk Assessment Facilitator leads the discussion through asset, threat, and vulnerability identification, the next task is to gather stakeholder estimates on the extent of the potential damage to the asset, regardless of the asset class definition. The extent of potential damage is defined as asset exposure.

As discussed previously, the Business Owner is responsible for both identifying assets and estimating potential loss to asset or the organization. As a review, the asset class, exposure, and the combination of threat and vulnerability define the overall impact to the organization. The impact is then combined with probability to complete the well-formed risk statement, as defined in Chapter 3.

The Risk Assessment Facilitator starts the discussion by using the following examples of qualitative categories of potential exposure for each threat and vulnerability combination associated with an asset:

- Competitive advantage
- Legal/regulatory
- Operational availability
- Market reputation

For each category, assist stakeholders in placing estimates within the following three groups:

- **High exposure.** Severe or complete loss of the asset
- **Moderate exposure.** Limited or moderate loss
- **Low exposure.** Minor or no loss

The prioritization section of this chapter provides guidance for adding detail to the exposure categories above. As with the task of quantifying assets, the Microsoft security risk management process recommends waiting until the risk prioritization step to further define exposure levels.

Note If stakeholders have difficulty selecting exposure levels during the facilitated discussions, expand on the threat and vulnerability details to help communicate the potential level of damage or loss to the asset. Public examples of security breaches are another useful tool. If additional help is needed, introduce the more detailed levels of exposure as defined in the detailed prioritization section later in this chapter.

Estimating Probability of Threats

After stakeholders have provided estimates for the potential impact to organizational assets, the Risk Assessment Facilitator collects the stakeholders' opinions on the probability of the impacts occurring. This brings closure to the risk discussion and helps the stakeholder to understand the thought process of identifying security risks. Recall that the Information Security Group owns the eventual decision on estimating the probability

of impacts occurring to the organization. This discussion can be viewed as a courtesy and a stakeholder goodwill builder.

Use the following guidelines to estimate probability for each threat and vulnerability identified in the discussion:

- **High.** Likely, one or more impacts expected within one year
- **Medium.** Probable, impact expected within two to three years
- **Low.** Not probable, impact not expected to occur within three years

Often this includes reviewing incidents that have occurred in the recent past. As appropriate, discuss these in order to help stakeholders understand the importance of security and the overall risk management process.

The Microsoft security risk management process associates a one-year timeframe to the high probability category because information security controls often take long periods to deploy. Selecting a probability within one year calls attention to the risk and encourages a mitigation decision within the next budgeting cycle. A high probability, combined with a high impact, forces a risk discussion across the stakeholders and the Security Risk Management Team. The Information Security Group must be aware of this responsibility when estimating the probability of impacts.

The next task is to gather stakeholder opinions on potential controls that may reduce the probability of identified impacts. Treat this discussion as a brainstorming session, and do not criticize or dismiss any ideas. Again, the primary purpose of this discussion is to demonstrate all components of risk to facilitate understanding. Actual mitigation selection occurs in the Conducting Decision Support phase. For each potential control identified, revisit the probability discussion to estimate the level of reduced occurrence using the same qualitative categories described previously. Point out to stakeholders that the concept of reducing the probability of risk is the primary variable for managing risk to an acceptable level.

Facilitating Risk Discussions

This section outlines risk discussion meeting preparations and defines the five tasks within the data gathering discussion (determining organizational assets and scenarios, identifying threats, identifying vulnerabilities, estimating asset exposure, identifying existing controls and the probability of an exploit).

Meeting Preparations

One subtle yet important success factor is the order in which risk discussions are held. Experience within Microsoft shows that the more information the Security Risk Management Team has going into each meeting, the more productive the meeting's outcome. One strategy is to build a knowledge base of risks across the organization to leverage the experience of the information security and IT teams. Meet with the Information Security Group first and then the IT teams in order to update your knowledge about the environment. This allows the Security Risk Management Team to have a greater understanding of each stakeholder's area of the organization. This also allows the Security Risk Management Team to share progress of the risk assessment with stakeholders as appropriate. Following this best practice, conduct any executive management risk discussions toward the end of the data gathering process. Executives often want an early view of the direction that the risk assessment is taking. Do not confuse this with executive sponsorship and support. Executive participation is required at the beginning and throughout the risk assessment process.

Invest time in building the list of invitees for each risk discussion. A best practice is to conduct meetings with groups of stakeholders with similar responsibilities and technical knowledge. The goal is to make attendees feel comfortable with the technical level of discussion. While a diverse set of stakeholders may benefit from hearing other views on organization risk, the risk assessment process must remain focused to collect all relevant data in the time allotted.

After you schedule risk discussions, research each stakeholder's area of the organization to become familiar with the assets, threats, vulnerabilities, and controls. As noted above, this information allows the Risk Assessment Facilitator to keep the discussion on track and at a productive pace.

Facilitating Discussions

The facilitated discussion should have an informal tone; however, the Risk Assessment Facilitator must keep the discussion moving in order to cover all relevant material. Experience shows that discussion often strays from the agenda. Likely pitfalls are when stakeholders initiate technical discussions surrounding new vulnerabilities or have preconceived control solutions. The Risk Assessment Facilitator should use the pre-meeting research and his or her expertise to capture a summary of the technical discussion and keep the meeting moving forward. With sufficient preparation, a meeting with four to six stakeholders should last approximately 60 minutes.

Invest a few minutes in the beginning to cover the agenda and highlight the roles and responsibilities across the risk management program. Stakeholders must clearly understand their roles and expected contributions. Another best practice is to provide all stakeholders with a sample risk discussion worksheet for personal note taking. This also provides a reference as the Risk Assessment Facilitator conducts the risk discussion. Another best practice is to arrive early and sketch the risk template on a white board to record data throughout the meeting. For a 60-minute meeting, the meeting timeline should resemble the following:

- Introductions and Risk Management Overview: 5 minutes
- Roles and Responsibilities: 5 minutes
- Risk Discussion: 50 minutes

The risk discussion is divided into the following sections:

- Determining Organizational assets and Scenarios
- Identifying Threats
- Identifying Vulnerabilities
- Estimating Asset Exposure
- Estimating Probability of Threats
- Proposed Control Discussions
- Meeting Summary and Next Steps

The actual flow of the meeting varies according to the group of participants, number of risks discussed, and experience of the Risk Assessment Facilitator. Use this as a guide in terms of the relative time investment for each task of the assessment. Also, consider sending the data gathering template before the meeting if stakeholders have previous experience with the risk assessment process.

Note The remaining sections of this chapter incorporate example information to help demonstrate the use of the tools referenced in the Assessing Risk phase. The example company is fictitious, and the risk related content represents only a fraction of the data required for a completed risk assessment. The focus of the example is simply to show how information can be

collected and analyzed by using the tools provided with this guide. A full demonstration of all aspects of the Microsoft security risk management process produces significant amounts of data and is out of scope for this guide. The fictitious company is a consumer retail bank called Woodgrove Bank. Content related to the example can be identified by the "Woodgrove Example" heading preceding each example topic.

Task One: Determining Organizational Assets and Scenarios

The first task is to collect stakeholder definitions of organizational assets within the scope of the risk assessment. Use the data gathering template, shown below, to populate tangible, intangible, or IT service assets as appropriate. (SRMGTool1-Data Gathering Tool.doc is also included as a tool with this guide.) For each asset, assist stakeholders in selecting an asset class and recording it in the template. As appropriate, also record the asset owner. If stakeholders have difficulty in selecting an asset class, verify that the asset is defined at a detailed level in order to facilitate discussion. If stakeholders continue to have difficulty, skip this task and wait until the threat and vulnerability discussions. Experience shows that stakeholders may have an easier time classifying assets when they realize the potential threats to the asset and the overall business.

The discussion surrounding organizational assets can be limited to a few simple questions. For example, is the asset critical to the success of the company, and can the asset have a material impact on the bottom line? If yes, the asset has the potential to cause a high impact to the organization.

Data Gathering Template

Identify assets that your group is responsible for developing, managing, supporting, or maintaining.

Asset Name	Asset Classification (High, Medium, or Low Business Impact)
1.	

For each asset, complete the following:

Defense-in-Depth Layer	What You Are Afraid of or Are Trying to Avoid: (Threats)	How It May Happen: (Vulnerabilities)	Exposure Level (H,M,L)	Current Controls Descriptions	Probability (H,M,L)	Control Concerns, Potential New Controls
Physical						
Application						
Host						
Network						
Data						

Figure 4.3: Snapshot of the Data Gathering Template (SRMGTool1)

Woodgrove Example Woodgrove Bank has many high value assets ranging from interest calculation systems and customer PII to consumer financial data and reputation as a trusted institution. This example focuses only on one of these assets—consumer financial data—in order to help demonstrate the use of the tools included with this guide. After discussing asset ownership in the risk discussion meeting, the Security Risk Management Team identified the Vice President of Consumer Services as the asset owner. If a controversial risk or expensive mitigation strategy is identified, this Business Owner will be a key stakeholder in deciding acceptable risk to Woodgrove Bank. While speaking with representatives of Consumer Services, the Security Risk Management Team confirmed that consumer financial data is a high business value asset.

Task Two: Identifying Threats

Use common terminology to facilitate discussion surrounding threats, for example what do stakeholders want to avoid happening to various assets? Focus discussions on what may happen versus how it may happen. Phrase questions in terms of the confidentiality, integrity, or availability of the asset, and record in the data gathering template.

Woodgrove Example Using the assets discussed previously, many threats may be identified. For brevity, this example focuses only on the threat of a loss of integrity to consumer financial

data. Additional threats may also exist surrounding the availability and confidentiality of consumer data; however, they are out of scope for this basic example.

Task Three: Identifying Vulnerabilities

For each threat identified, brainstorm vulnerabilities, for example, how the threat may occur. Encourage stakeholders to give specific technical examples when documenting vulnerabilities. Each threat may have multiple vulnerabilities. This is expected and assists in the later stages of identifying controls in the Conducting Decision Support phase of the risk management process.

Woodgrove Example Considering the threat of a loss of integrity to consumer financial data, the Security Risk Management Team condensed information gathered during the risk discussions into the following three vulnerabilities:

- Theft of financial advisor credentials by trusted employee abuse using non-technical attacks, for example, social engineering or eavesdropping.
- Theft of financial advisor credentials off local area network (LAN) hosts through the use of outdated security configurations.
- Theft of financial advisor credentials off remote, or mobile, hosts as a result of outdated security configurations.

Note There may be many more vulnerabilities in this scenario. The goal is to demonstrate how vulnerabilities are assigned to specific threats. Also note that the stakeholders may not articulate vulnerabilities in technical terms. The Security Risk Management Team must refine threat and vulnerability statements as needed.

Task Four: Estimating Asset Exposure

The Risk Assessment Facilitator leads the discussion to estimate exposure for every threat and vulnerability combination. Ask stakeholders to select a high, moderate, or low exposure level and record in the template. For digital assets and systems, a helpful guideline is to classify exposure as high if the vulnerability allows administrative, or root, level control of the asset.

Woodgrove Example After the threats and vulnerabilities are identified, the Risk Assessment Facilitator leads the discussion to collect information on the potential level of damage that the previously-discussed threat and vulnerability combinations may have on the business. After some discussion, the group determines the following:

- A breach of integrity through trusted employee abuse may be damaging to the business, but probably not severely so. Extent of damage is limited in this scenario because each financial advisor can only access customer data that he or she manages. Thus, the discussion group recognizes that a smaller number of stolen credentials would do less damage than a larger number.
- A breach of integrity through credential theft on LAN hosts could cause a severe, or High, level of damage. This is especially true of an automated attack that could collect multiple financial advisor credentials in a short period of time.
- A breach of integrity through credential theft on mobile hosts could also have a severe, or High, level of damage. The discussion group notes that the security configurations on remote hosts often lag behind LAN systems.

Task Five: Identifying Existing Controls and Probability of Exploit

Use the risk discussion to better understand stakeholders' views of the current control environment, their opinions on the probability of an exploit, and their suggestions for proposed controls. Stakeholder perspectives may vary from actual implementation but provide a valuable reference to the Information Security Group. Use this point in the

discussion to remind stakeholders of their roles and responsibilities within the risk management program. Document the results in the template.

Woodgrove Example After the discussion on the possible exposure to the company with the identified threats and vulnerabilities, the non-technical stakeholders do not have sufficient experience to comment on the probability of one host being compromised over another. However, they do agree that their remote hosts, or mobile hosts, do not receive the same level of management as those on the LAN. There is discussion on requiring financial advisors to periodically review activity reports for unauthorized behavior. This feedback is collected and will be considered by the Security Risk Management Team during the Conducting Decision Support phase.

Summarizing the Risk Discussion

At the end of the risk discussion, briefly summarize the risks identified to help bring closure to the meeting. Also, remind stakeholders of the overall risk management process and timeline. The information gathered in the risk discussion gives stakeholders an active role in the risk management process and provides valuable insight for the Security Risk Management Team.

Woodgrove Example The Risk Assessment Facilitator summarizes the discussion and highlights the assets, threats, and vulnerabilities discussed. He or she also describes the larger risk management process and educates the discussion group on the fact that the Security Risk Management Team will incorporate its input, and the input of others, when estimating the probability of each threat and vulnerability.

Defining Impact Statements

The last task in the facilitated data gathering step is to analyze the potentially large amount of information collected throughout the risk discussions. The output of this analysis is a list of statements describing the asset and the potential exposure from a threat and vulnerability. As defined in Chapter 3, these statements are called impact statements. The impact is determined by combining the asset class with the level of potential exposure to the asset. Recall that impact is one half of the larger risk statement; impact is combined with the probability of occurrence to complete a risk statement.

The Security Risk Management Team creates the impact statements by consolidating information gathered in risk discussions, by incorporating any previously identified impacts, and also by including impact data from its own observations. The Security Risk Management Team is responsible for this task but should request additional information from stakeholders as needed.

The impact statement contains the asset, asset classification, defense-in-depth layer, threat description, vulnerability description, and exposure rating. Use the information collected in the data gathering template to define impact statements for all facilitated discussions. Figure 4.4 shows the applicable column headings in the Summary Level Risk template to collect impact specific data.

Information Collected During Data Gathering Process							
Asset				Exposure			
Date Identified	Asset Name/Desc.	Asset Class	Applicable Defense-in-Depth Layer(s)	Threat Description	Vulnerability Description	Exposure Rating (H,M,L)	Impact Rating (H,M,L)

Figure 4.4: Summary Risk Level Worksheet: Asset and Exposure Columns (SRMGTool2)

Woodgrove Example The sample information collected during the risk discussions can be organized by developing impact statements. The Security Risk Management Team may document the impact statements in a sentence format; for example, "The integrity of high value customer data may be compromised from credential theft of remotely managed hosts." While this approach is accurate, writing sentences does not scale to a large number of risks due to inconsistencies in writing, understanding, and the lack organizing data (sorting or querying risks). A more efficient approach is to populate the impact data into the Summary Level table as shown below.

Asset				Exposure			Impact Rating (H,M,L)
Date Identified	Asset Name	Asset Class	Applicable Defense-in-Depth Layer(s)	Threat Description	Vulnerability Description	Exposure Rating (H,M,L)	
Date	Consumer financial investment data	HBI	Host	Unauthorized access to consumer data through theft of Financial Advisor credentials	Theft of credentials off managed LAN client via outdated configuration of antivirus signatures, host configuration, or outdated security patches	M	H
Date	Consumer financial investment data	HBI	Host	Unauthorized access to consumer data through theft of Financial Advisor credentials	Theft of credentials off managed, remote client via outdated configuration of antivirus signatures, host configuration, or outdated security patches	M	H
Date	Consumer financial investment data	HBI	Data	Unauthorized access to consumer data through theft of Financial Advisor credentials	Theft of credentials by trusted employee abuse via non-technical attacks, e.g. social engineering or eavesdropping	L	M

Figure 4.5: Woodgrove Example: Information Collected During Data Gathering Process (SRMGTool2)

Note The next section, titled "Risk Prioritization," provides additional guidance on selecting and documenting the impact rating used in the Summary Level Risk process.

Data Gathering Summary

By consolidating the information collected in the data gathering discussions into individual impact statements, the Security Risk Management Team has completed the tasks in the facilitated data gathering step of the Assessing Risk phase. The next section, "Risk Prioritization," details the tasks involved in risk prioritization. During prioritization, the Security Risk Management Team is responsible for estimating the probability for each impact statement. The Security Risk Management Team then combines the impact statements with their estimates for probability of occurrence. The result is a comprehensive list of prioritized risks, which completes the Assessing Risk phase.

When you analyze risks, you may identify risks that are dependent on another risk occurring. For example, if an escalation of privilege occurs to a low business impact

asset, a high business impact asset may then be exposed. Although this is a valid exercise, risk dependencies can become extremely data intensive to collect, track, and manage. The Microsoft security risk management process recommends highlighting dependencies, but it is not usually cost effective to actively manage all of them. The overall goal is to identify and manage the highest priority risks to the business.

Risk Prioritization

As discussed in the previous section, the facilitated data gathering step defines the tasks to produce a list of impact statements for identifying organizational assets and their potential impacts. This section addresses the next step in the Assessing Risk phase: risk prioritization. The prioritization process adds the element of probability to the impact statement. Recall that a well formed risk statement requires both the *impact* to the organization and the *probability* of that impact occurring. The prioritization process can be characterized as the last step in "defining which risks are most important to the organization." Its end result is a prioritized list of risks that will be used as the inputs in the decision support process that Chapter 5, "Conducting Decision Support," discusses.

The Information Security Group is the sole owner of the prioritization process. The team may consult technical and non-technical stakeholders, but it is accountable for determining the probability of potential impacts to the organization.

By applying the Microsoft security risk management process, the level of probability has the potential to raise the awareness of a risk to the highest levels of the organization, or it can drop awareness so low that the risk may be accepted without further discussion. Estimating risk probability requires the Security Risk Management Team to invest significant time in order to thoroughly evaluate each priority threat and vulnerability combination. Each combination is assessed against current controls to consider the effectiveness of those controls influencing the probability of impact to the organization. This process can be overwhelming for large organizations and may challenge the initial decision to invest in a formal risk management program. To reduce the amount of time invested in prioritizing risks, you may consider separating the process into two tasks: a summary level process and a detailed level process.

The summary level process produces a list of prioritized risks very quickly, analogous to the triage procedures that hospital emergency rooms use to ensure that they help the patients in greatest need first. However, the drawback is that it yields a list containing only high-level comparisons between risks. A long, summary level list of risks in which each risk is categorized as high does not provide sufficient guidance to the Security Risk Management Team or allow the team to prioritize mitigation strategies. Nevertheless, it allows teams to quickly triage risks in order to identify the high and moderate risks, which enables the Security Risk Management Team to focus its efforts on only the risks deemed most important.

The detailed level process produces a list with more detail, more easily distinguishing risks one from another. The detailed risk view enables stack-ranking of risks and also includes a more detailed view of the potential financial impact from the risk. This quantitative element facilitates cost of control discussions in the decision support process, which the next chapter details.

Some organizations may choose not to produce a summary level risk list at all. Without consideration, it may seem that this strategy would save time up front, but this is not the case. Minimizing the number of risks in the detailed level list ultimately makes the risk assessment process more efficient. A primary goal of the Microsoft security risk management process is to simplify the risk assessment process by striking a balance between added granularity for risk analysis and the amount of effort required to calculate

risk. Simultaneously, it endeavors to promote and preserve clarity regarding the logic involved so that stakeholders possess a clear understanding of risks to the organization.

Some risks may have the same risk ranking in both the summary list and the detailed list; however, the rankings still provide sufficient details to determine whether the risk is important to the organization and if it should proceed to the decision support process.

Note The ultimate goal of the Assessing Risk phase is to define the most important risks to the organization. The goal of the Conducting Decision Support phase is then to determine what should be done to address them.

Teams often become stalled at this stage while stakeholders debate the importance of various risks. To minimize possible delays, apply the following tasks as appropriate for your organization:

1. In non-technical terms, define high and medium level risks for your organization before starting the prioritization process.
2. Focus attention on risks that are on the border between medium and high levels.
3. Avoid discussing how to address risks before you have decided whether the risk is important. Be watchful for stakeholders who may have preconceived solutions in mind and are looking for risk findings to provide project justification.

The remainder of this section discusses success factors and tasks for creating summary and detailed level risk rankings. The following tasks and Figure 4.6 below provide an overview of the section and key deliverables throughout the risk prioritization process.

Primary Tasks and Deliverables

- **Task one.** Build the summary level list using broad categorizations to estimate probability of impact to the organization.
 - *Output.* Summary level list to quickly identify priority risks to the organization.
- **Task two.** Review summary level list with stakeholders to begin building consensus on priority risks and to select the risks for the detailed level list.
- **Task three.** Build the detailed level list by examining detailed attributes of the risk in the current business environment. This includes guidance to determine a quantitative estimate for each risk.
 - *Output.* Detailed level list providing a close look at the top risks to the organization.

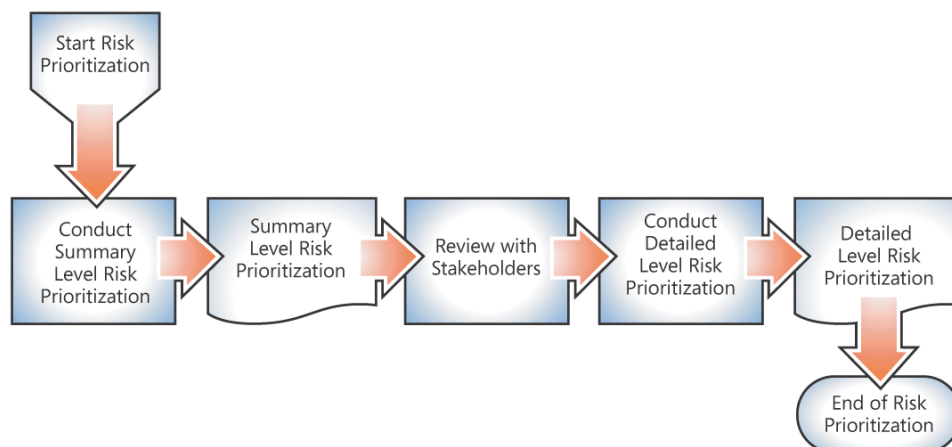


Figure 4.6: Risk Prioritization Tasks

Note The detailed level risk output will be reviewed with stakeholders in the decision support process discussed in Chapter 5.

Preparing for Success

Prioritizing risks to the organization is not a simple proposition. The Security Risk Management Team must attempt to predict the future by estimating when and how potential impacts may affect the organization, and it then must justify those predictions to stakeholders. A common pitfall for many teams is "hiding" the tasks involved with determining probability and using calculations to represent probability in terms of percentages or other bottom-line figures to which they assume Business Owners will more readily respond. But experience in developing the Microsoft security risk management process has proven that stakeholders are more likely to accept the Security Risk Management Team's analyses if the logic is clear during the prioritization process. The process maintains focus on stakeholder understanding throughout the process. You should keep the prioritization logic as simple as possible in order to reach consensus quickly while minimizing misunderstandings. Experience conducting risk assessments within Microsoft IT and other enterprises shows the following best practices also help the Security Risk Management Team during the prioritization process:

- Analyze risks during the data gathering process. Because risk prioritization can be time intensive, try to anticipate controversial risks and start the prioritization process as early as possible. This shortcut is possible because the Security Risk Management Team is the sole owner of the prioritization process.
- Conduct research to build credibility for estimating probability. Use past audit reports and consider industry trends and internal security incidents as appropriate. Revisit stakeholders as needed to learn about the current controls and awareness of specific risks in their environments.
- Schedule sufficient time in the project to conduct research and perform analysis of the effectiveness and capabilities of the current control environment.
- Remind stakeholders that the Security Risk Management Team has the responsibility of determining probability. The executive sponsor must also acknowledge this role and support the analysis of the Security Risk Management Team.
- Communicate risk in business terms. Avoid any tendency to use language related to fear or technical jargon in the prioritization analysis. The Security Risk Management Team must communicate risk in terms that the organization understands while resisting any temptation to exaggerate the degree of danger.
- Reconcile new risks with previous risks. While creating the summary level list, incorporate risks from previous assessments. This allows the Security Risk Management Team to track risks across multiple assessments and provides an opportunity to update previous risk elements as needed. For example, if a previous risk was not mitigated due to high mitigation costs, revisit the probability of the risk occurring and review and reconsider any changes to the mitigation solution or costs.

Prioritizing Security Risks

The following section explains the process of developing the summary and detailed level risk lists. It may be helpful to print out the supporting templates for each process located in the tools section.

Conducting Summary Level Risk Prioritization

The summary level list uses the impact statement produced during the data gathering process. The impact statement is the first of two inputs in the summary view. The second

input is the probability estimate determined by the Security Risk Management Team. The following three tasks provide an overview of the summary level prioritization process:

- **Task one.** Determine impact value from impact statements collected in the data gathering process.
- **Task two.** Estimate the probability of the impact for the summary level list.
- **Task three.** Complete the summary level list by combining the impact and probability values for each risk statement.

Task One: Determine Impact Level

The asset class and asset exposure information collected in the data gathering process must be summarized into a single value to determine impact. Recall that impact is the combination of the asset class and the extent of exposure to the asset. Use the following figure to select the impact level for each impact statement.

Impact Rating Reference				
Asset Class	High	Moderate	High	High
	Med	Low	Moderate	High
	Low	Low	Low	Moderate
		Low	Medium	High
Exposure Level				

Figure 4.7: Risk Analysis Worksheet: Asset Class and Exposure Level (SRMGTool2)

Woodgrove Example Recall that the Woodgrove example had three impact statements. The following list summarizes these statements by combining the asset class and exposure level:

- **Trusted Employee Theft Impact:** HBI asset class and Low Exposure. Using the figure above, this leads to a Moderate Impact.
- **LAN Host Compromise Impact:** HBI asset class and High Exposure lead to High Impact.
- **Remote Host Compromise Impact:** HBI asset class and High Exposure lead to High Impact.

Task Two: Estimate Summary Level Probability

Use the same probability categories discussed in the data gathering process. The probability categories are included below for reference:

- **High.** Likely, one or more impacts expected within one year
- **Medium.** Probable, impact expected at least once within two to three years
- **Low.** Not probable, impact not expected to occur within three years

Woodgrove Example The Summary Level Risk Prioritization is the first formal documentation of the Security Risk Management Team's estimate on risk probability. The Security Risk Management Team should be prepared to provide evidence or anecdotes justifying their estimates, for example, reciting past incidents or referencing current control effectiveness. The following list summarizes the probability levels for the Woodgrove example:

- **Trusted Employee Theft Probability: Low.** Woodgrove National Bank prides itself on hiring trusted employees. Management verifies this trust with background checks and conducts random audits of Financial Advisor activity. There have been no incidents of employee abuse identified in the past.
- **LAN Host Compromise Probability: Medium.** The IT department recently formalized its patch and configuration process on the LAN due to inconsistencies in previous years. Because

tailor the Microsoft security risk management process, including the tools, to meet your individual needs.

Woodgrove Example The following figure completes the example of the summary level risk list for Woodgrove Bank. Note that the columns of "Probability" and "Summary Risk Level" have been added to the impact statement information to complete the elements of a well-formed risk statement.

Information Collected During Data Gathering Process						
Asset				Exposure		
Date Identified	Asset Name	Asset Class	Applicable Defense-in-Depth Layer(s)	Threat Description	Vulnerability Description	Exposure Rating
example	Consumer financial investment data	HBI	Host	Unauthorized access to consumer data through theft of Financial Advisor credentials	Theft of credentials off managed LAN client via outdated configuration of antivirus signatures, host configuration, or outdated security patches	M
example	Consumer financial investment data	HBI	Host	Unauthorized access to consumer data through theft of Financial Advisor credentials	Theft of credentials off managed, remote client via outdated configuration of antivirus signatures, host configuration, or outdated security patches	M
example	Consumer financial investment data	HBI	Data	Unauthorized access to consumer data through theft of Financial Advisor credentials	Theft of credentials by trusted employee abuse via non-technical attacks, e.g. social engineering or eavesdropping	L

Description	Exposure Rating (H,M,L)	Impact Rating (H,M,L)	Probability (H,M,L)	Summary Risk Level (H,M,L)
Unauthorized access to consumer data through theft of Financial Advisor credentials off managed LAN client via outdated configuration of antivirus signatures, host configuration, or outdated security patches	M	H	M	H
Unauthorized access to consumer data through theft of Financial Advisor credentials off managed, remote client via outdated configuration of antivirus signatures, host configuration, or outdated security patches	M	H	H	H
Unauthorized access to consumer data through theft of Financial Advisor credentials by trusted employee abuse via non-technical attacks, e.g. social engineering or eavesdropping	L	M	L	L

Figure 4.10: Woodgrove Bank Example of Summary Level Risk List (SRMGTool2)

Reviewing with Stakeholders

The next task in the prioritization process is to review the summary results with stakeholders. The goals are to update stakeholders about the risk assessment process and solicit their input to help select which risks to conduct a detailed level analysis. Use the following criteria when selecting risks to include in the detailed level prioritization process:

- **High level risks.** Every risk rated as high must be included on the detailed list. Each high risk must have a resolution after the decision support process, for example, accept the risk or develop a mitigation solution.
- **Borderline risks.** Create the detailed prioritization analysis for moderate risks that require a resolution. In some organizations, even all moderate risks may be included in the detailed list.
- **Controversial risks.** If a risk is new, not well understood, or viewed differently by stakeholders, create the detailed analysis to help stakeholders achieve a more accurate understanding of the risk.

Woodgrove Example Note that the "Trusted Employee Theft" risk is rated as Low in the summary level risk list. At this point in the prioritization process, this risk is well understood by all stakeholders. In the Woodgrove example, this risk serves as an example of a risk that does not need to graduate to the detailed level risk prioritization step. For the remainder of the Woodgrove example, only the LAN and remote host compromise risks are prioritized.

Conducting Detailed Level Risk Prioritization

Producing the detailed level risk list is the last task in the risk assessment process. The detailed list is also one of the most important tasks because it enables the organization to understand the rationale behind the most important risks to the company. After you complete the risk assessment process, sometimes simply communicating a well documented risk to stakeholders is sufficient enough to trigger action. For organizations without a formal risk management program, the Microsoft security risk management process can be an enlightening experience.

Note If a risk is well understood by all stakeholders, the summary level detail may be sufficient to determine the appropriate mitigation solution.

The detailed risk list leverages many of the inputs used in the summary level list; however, the detailed view requires the Security Risk Management Team to be more specific in its impact and probability descriptions. For each summary level risk, verify that each threat and vulnerability combination is unique across risks. Often summary level risks may not be described sufficiently to be associated with specific controls in the environment; if this happens, you may not be able to accurately estimate probability of occurrence. For example, you can improve upon the threat description in the following summary level risk statement to describe two separate risks:

- **Summary level risk statement.** Within one year, high value servers may be moderately impacted from a worm due to unpatched configurations.
- **Detailed level statement 1.** Within one year, high value servers may be unavailable for three days due to worm propagation caused by unpatched configurations.
- **Detailed level statement 2.** Within one year, high value servers may be compromised, affecting the integrity of data due to worm propagation caused by unpatched configurations.

Note As a best practice, become familiar with the detailed risk analysis before the data gathering process. This helps the Security Risk Management Team ask specific questions during the initial data gathering discussions with stakeholders and minimizes the need for follow-up meetings.

The detailed level risk list also requires specific statements on the effectiveness of the current control environment. After the Security Risk Management Team has attained detailed understanding of the threats and vulnerabilities affecting the organization, work can begin on understanding the details of current controls. The current control environment determines the probability of potential risks to the organization. If the control environment is sufficient, then the probability of a risk to the organization is low. If the control environment is insufficient, a risk strategy must be defined—for example, accept the risk, or develop a mitigation solution. As a best practice, risks should be tracked regardless of final risk level. For example, if the risk is deemed acceptable, save this information for future assessments.

The last element of the detailed level risk list is an estimate of each risk in quantifiable, monetary terms. Selecting a monetary value for risk does not occur until work has begun on the detailed level list because of the time required to build consensus across the stakeholders. The Security Risk Management Team may need to revisit stakeholders to collect additional data.

The following four tasks outline the process to build a detailed level list of risks. You might find it helpful to print out the template in the Tools section titled "SRMGTool3-Detailed Level Risk Prioritization.xls." The output is a detailed list of risks affecting the current organization. The quantitative estimate is determined after the detailed risk value and is described in the next section.

- **Task one.** Determine impact and exposure.
- **Task two.** Identify current controls.

- **Task three.** Determine probability of impact.
- **Task four.** Determine detailed risk level.

Task One: Determine Impact and Exposure

First, insert the asset class from the summary table into the detailed template. Next, select the exposure to the asset. Notice that the exposure rating in the detailed template contains additional granularity compared to the summary level. The exposure rating in the detailed template consists of a value from 1-5. Recall that the exposure rating defines the extent of damage to the asset. Use the following templates as a guide to determine the appropriate exposure rating for your organization. Because each value in the exposure figures may affect the level of impact to the asset, insert the highest of all values after you populate the figures. The first exposure figure assists in measuring the extent of impact from a compromise of the confidentiality or integrity of business assets. The second figure assists in measuring the impact on the availability of assets.

Exposure Rating	Confidentiality or Integrity of Asset
5	Severe or complete damage to asset, e.g. externally visible and affects business profitability or success
4	Serious but not complete damage to asset, e.g. affects business profitability or success, may be externally visible
3	Moderate damage or loss, e.g. affects internal business practices, causes increase in operational costs or reduction of revenue
2	Low damage or loss, e.g. affects internal business practices, cannot measure increase in costs
1	Minor or no change in asset

Figure 4.11: Risk Analysis Worksheet: Confidentiality or Integrity Exposure Ratings (SRMGTool3)

After considering the extent of damage from potential impacts to confidentiality and integrity, use the following figure to determine the level of impact from the lack of availability to the asset. Select the highest value as the exposure level from both tables.

Exposure Rating	Availability	Description
5	Work stoppage	Substantial support costs or business commitments canceled.
4	Work interruption	Quantifiable increase in support costs or business commitments delayed.
3	Work delays	Noticeable impact to support costs and productivity. No measurable business impact.
2	Work distraction	No measurable impact, minor increases in support or infrastructure costs.
1	Absorbed by normal business operations	No measurable impact to support costs, productivity, or business commitments.

Figure 4.12: Risk Analysis Worksheet: Availability Exposure Ratings (SRMGTool3)

Use the figure as a guide to collect exposure ratings for each potential impact. If the data gathering discussions did not provide sufficient detail on the possible exposure levels, you may need to review them with the specific asset owner. As mentioned in the data gathering section, reference the above exposure descriptions during the risk discussions as needed.

Woodgrove Example The following list summarizes the exposure ratings for the two remaining risks:

- **LAN Host Compromise Exposure Rating: 4.** The business impact may be serious and externally visible, but it should not completely damage all consumer financial data. Thus, a rating of 4 is selected.
- **Remote Host Compromise Exposure Rating: 4.** (Same as above).

After the exposure rating is identified, you are ready to determine the impact value by filling in the appropriate columns in SRMGTool3-Detailed Risk Level Prioritization.xls and calculating the value. In the detailed level risk process, impact is the product of the impact class value and the exposure factor. Each exposure rating is assigned a percentage that reflects the extent of damage to the asset. This percentage is called the exposure factor. The Microsoft security risk management process recommends a linear scale of 100 percent exposure to 20 percent; adjust accordingly to your organization. Each impact value is also associated with a qualitative value of high, medium, or low. This classification is helpful for communicating the impact level and tracking the risk elements throughout the detailed risk calculations. As an aid, the following figure also shows the possible impact values for each impact class.

Impact class	Impact Class Value (V)
HBI	10
MBI	5
LBI	2

Exposure Factor Rating	Exposure Factor (EF)	Impact Rating (V * EF)	Impact Range	Summary Level Comparison
5	100%		7 - 10	High
4	80%		4 - 6	Medium
3	60%		0 - 3	Low
2	40%			
1	20%			

Figure 4.13: Risk Analysis Worksheet: Determining Impact Values (SRMGTool3)

Woodgrove Example The following figure shows how the impact class values, exposure rating, and overall impact rating are determined by using the Woodgrove example.

Asset		Exposure				
Asset Name	Impact Class Rating	Defense-in-Depth Layer	Threat Description	Vulnerability Description	Exposure Rating (1-5)	Impact Rating (1-10)
Consumer financial investment data	10 (HBI)	Host	Unauthorized access to consumer data through theft of Financial Advisor credentials	Theft of credentials off managed LAN client via outdated configuration of antivirus signatures, host configuration, or outdated security patches	4 (80%)	8
Consumer financial investment data	10 (HBI)	Host	Unauthorized access to consumer data through theft of Financial Advisor credentials	Theft of credentials off managed remote client via outdated configuration of antivirus signatures, host configuration, or outdated security patches	4 (80%)	8

Figure 4.14: Woodgrove Example Showing Detailed Values Impact Class, Exposure Rating, and Impact Value (SRMGTool3)

Task Two: Identify Current Controls

SRMGTool3-Detailed Risk Level Prioritization.xls describes the current controls in the organization that currently reduce the probability of the threat and vulnerability defined in the impact statement. A control effectiveness rating is also evaluated in the detailed probability calculations; however, documenting applicable controls assists when communicating risk elements. It may be helpful to organize the control descriptions into the well-known categories of management, operations, or technical control groups. This information is also useful in the decision support process described in Chapter 5.

Woodgrove Example The following represents a sample list of primary controls for the "LAN host compromise risk." See the SRMGTool3-Detailed Risk Level Prioritization.xls for additional control descriptions. Note that the control descriptions can also be used to help justify exposure ratings:

- Financial Advisors can only access accounts they own; thus, the exposure is less than 100 percent.
- E-mail notices to patch or update hosts are proactively sent to all users.
- The status of antivirus and security updates are measured and enforced on the LAN every few hours. This control reduces the time window when LAN hosts are vulnerable to attack.

Task Three: Determine Probability of Impact

The probability rating consists of two values. The first value determines the probability of the vulnerability existing in the environment based on attributes of the vulnerability and possible exploit. The second value determines the probability of the vulnerability existing based on the effectiveness of current controls. Each value is represented by a range of 1-5. Use the following figures as guides to determine the probability of each impact to the organization. The probability rating will then be multiplied by the impact rating to determine the relative risk rating.

Note Figures 4.15 and 4.17 were used to help Microsoft IT understand the probabilities of risks occurring in its environments. Adjust the contents as appropriate for your organization.

The Information Security Group owns the prioritization process and should tailor the prioritization attributes as needed. For example, you could modify the figures to focus on application specific vulnerabilities versus enterprise infrastructure vulnerabilities if the assessment scope focused on application development. The goal is to have a consistent collection of criteria for evaluating risk in your environment.

The following figure includes these vulnerability attributes:

- **Attacker population.** The probability of exploit normally increases as the attacker population increases in size and technical skill level.
- **Remote vs. local access.** The probability normally increases if a vulnerability can be exploited remotely.
- **Visibility of exploit.** The probability normally increases if an exploit is well known and publicly available.
- **Automation of exploit.** The probability normally increases if an exploit can be programmed to automatically seek out vulnerabilities across large environments.

Recall that estimating the probability of an exploit is subjective in nature. Use the above attributes as a guide to determine and justify probability estimates. The Security Risk Management Team must rely on and promote its expertise in selecting and justifying its predictions.

Probability Definitions for Vulnerabilities	
High	
<i>Large attacker population- "script-kiddie"/hobbyist</i>	
<i>Remotely executable</i>	
<i>Anonymous privileges needed</i>	
<i>Externally-published exploitation method</i>	
<i>Automated</i>	
"5" if any apply	
Medium	
<i>Medium attacker population - expert/specialist</i>	
<i>Non-remotely executable</i>	
<i>User level privileges required</i>	
<i>Not publicly-published exploitation method</i>	
<i>Non-automated</i>	
"3" if any apply	
Low	
<i>Small attacker population - insider knowledge</i>	
<i>Non-remotely executable</i>	
<i>Administrator level privileges required</i>	
<i>Not publicly-published exploitation method</i>	
<i>Non-automated</i>	
"1" if all apply	

Figure 4.15: Risk Analysis Worksheet: Evaluating Vulnerability (SRMGTool3)

Select the appropriate rating in the following figure.

Vulnerability sum:	
Exposure attributes (select one from above)	
high	5
medium	3
low	1
probability value (1, 3, or 5)	

Figure 4.16: Risk Analysis Worksheet: Evaluating Probability Value (SRMGTool3)

Woodgrove Example For the LAN and remote hosts, it is likely that all vulnerability attributes in the High category will be seen inside and outside Woodgrove's LAN environment in the near future. Thus, the vulnerability value is 5 for both risks.

The next figure evaluates the effectiveness of current controls. This value is subjective in nature and relies on the experience of the Security Risk Management Team to understand its control environment. Answer each question, and then total the values to determine the final control rating. A lower value means that the controls are effective and may reduce the probability of an exploit occurring.

How effective are current controls?	
Yes - 0, No - 1	
Is accountability defined and enforced effectively?	1,0
Is awareness communicated and followed effectively?	1,0
Are processes defined and practiced effectively?	1,0
Do existing technology or controls reduce threat effectively?	1,0
Are current audit practices sufficient to detect abuse or control deficiencies?	1,0
Sum of control attributes (0-5) =	

Figure 4.17: Risk Analysis Worksheet: Evaluating Current Control Effectiveness (SRMGTool3)

Woodgrove Example To show how the control effectiveness values can be used, the following table summarizes the values for the LAN host compromise risk only; see the SRMGTool3-Detailed Risk Level Prioritization.xls for the complete example:

Table 4.2. Woodgrove Example. Control Effectiveness Values

Control Effectiveness Question	Value	Description
Is accountability defined and enforced effectively?	0 (yes)	Policy creation and host compliance accountability are well defined.
Is awareness communicated and followed effectively?	0 (yes)	Regular notifications are sent to users and general awareness campaigns are conducted.
Are processes defined and practiced effectively?	0 (yes)	Compliance measurement and enforcement is documented and followed.
Does existing technology or controls reduce threat effectively?	1 (no)	Existing controls still allow a length of time between vulnerable and patched.
Are current audit practices sufficient to detect abuse or control deficiencies?	0 (yes)	Measurement and compliance auditing are effective given current tools.
Sum of all control attributes:	1	

Next, add the value from the Vulnerability figure (Figure 4.16) to the value from the Current Control figure (Figure 4.17) and insert into the detailed level template. The template is shown in the following figure for reference.

Sum of vulnerability rating AND control effectiveness (0-10) =	
--	--

Figure 4.18: Risk Analysis Worksheet: Probability Rating with Control (SRMGTool3)

Woodgrove Example The total probability rating for the LAN host example is 6 (value of 5 for the vulnerability, plus a value of 1 for control effectiveness).

Task Four: Determine Detailed Risk Level

The following figure displays the detailed level summary to identify the risk level for each risk identified. While assessing risk at a detailed level may seem complicated, the logic behind each task in the risk rating can be referenced using the previous figures. This ability to track each task in the risk statement provides significant value when helping stakeholders understand the underlying details of the risk assessment process.

Baseline Risk (Current)					
Asset		Exposure			
Asset Name	Impact Class Rating	Defense-in-Depth Layer	Threat Description	Vulnerability Description	Exposure Rating (1-5)
Description of digital asset to business.	Impact Class Rating, see Group definition tab (10,5,2).	Technical area(s) where exposure occurs: appl, host, net, data.	Storyline of what threat you are afraid of or are trying to avoid, e.g. hacker modifying data.	Storyline of how a threat may occur, e.g. hacker modified data by injecting a format string to execute an SQL command.	Exposure Rating, see Rating definition tab (1-5).

Asset	Exposure Rating (1-5)	Impact Rating (1-10)	Current Controls Description	Probability Rating w/Control (1-10)	Risk Rating w/Control (0-100)
Asset Name	Exposure Rating, see Rating definition tab (1-5).	The level of damage to the asset through the defined exposure. Product of Asset and Exposure values.	Current people, processes, or technologies to reduce the probability of the impact occurring.	Probability of the exposure succeeding to impact the asset with current controls (see ratings definitions).	Overall impact on business given the asset and probability of an exposure. Product of impact and probability rating.

Figure 4.19: Risk Analysis Worksheet: Establishing the Detailed Risk Level (SRMGTool3)

Woodgrove Example The following figure displays the Detailed Risk List example for Woodgrove Bank. This data is also presented in SRMGTool3.

Baseline Risk (Current)									
Asset		Exposure							
Asset Name	Impact Class Rating	Defense-in-Depth Layer	Threat Description	Vulnerability Description	Exposure Rating (1-5)	Impact Rating (1-10)	Current Controls Description	Probability Rating w/Control (1-10)	Risk Rating w/Control (0-100)
Consumer financial investment data	10 (HBI)	Host	Unauthorized access to consumer data through theft of Financial Advisor credentials	Theft of credentials off managed LAN client via outdated configuration of antivirus signatures, host configuration, or outdated security patches	4 (80%)	8	1. Each Advisor limited to own accounts, thus exposure < 100%. 2. Email notices to patch/update. 3. Antivirus update and patches enforced on LAN every few hours - narrowing compromise of host during time window of exploit vs. patch.	Vulnerability: 5 Control: 1 Total = 6	48
Consumer financial investment data	10 (HBI)	Host	Unauthorized access to consumer data through theft of Financial Advisor credentials	Theft of credentials off managed remote client via outdated configuration of antivirus signatures, host configuration, or outdated security patches	4 (80%)	8	1. Each Advisor limited to own accounts, thus exposure < 100%. 2. E-mail notices to patch/update. - No solution to ensure compliance outside of LAN connectivity.	Vulnerability: 5 Control: 5 Total = 10	80

Figure 4.20: Woodgrove Bank Example for Detailed Risk List (SRMGTool3)

The previous figure displays the contents of the risk rating and its data elements. As noted above, the risk rating is the product of the impact rating (with values ranging from 1-10) and the probability rating (with values ranging from 0-10). This produces a range of values from 0-100. By applying the same logic used in the summary level risk list, the detailed risk level can also be communicated in the qualitative terms of high, medium, or low. For example, a medium impact and a high probability produce a risk rating of high.

However, the detailed level list provides added specificity for each risk level, as shown in the following figure.

Impact rating * Probability rating = Risk Level													
Impact Rating Ranges		*	Probability Ranges										
High	10 -- 7		10 -- 7										
Medium	6 -- 4		6 -- 3										
Low	3 -- 0		3 -- 0										
Impact	H	10	0	10	20	30	40	50	60	70	80	90	100
		9	0	9	18	27	36	45	54	63	72	81	90
		8	0	8	16	24	32	40	48	56	64	72	80
		7	0	7	14	21	28	35	42	49	56	63	70
		6	0	6	12	18	24	30	36	42	48	54	60
	M	5	0	5	10	15	20	25	30	35	40	45	50
		4	0	4	8	12	16	20	24	28	32	36	40
		3	0	3	6	9	12	15	18	21	24	27	30
		2	0	2	4	6	8	10	12	14	16	18	20
	L	1	0	1	2	3	4	5	6	7	8	9	10
		0	1	2	3	4	5	6	7	8	9	10	
		L				M				H			
Probability													

Overall Risk	Risk level
41-100	High
20-40	Medium
0-19	Low

Figure 4.21: Risk Analysis Worksheet: Establishing the Summary Qualitative Ranking (SRMGTool3)

Use the detailed risk levels as a guide only. As discussed in Chapter 3, the Security Risk Management Team should be able to communicate to the organization, in writing, the meaning of high, medium, and low risks. The Microsoft security risk management process is simply a tool for identifying and managing risks across the organization in a consistent and repeatable way.

Quantifying Risk

As discussed in Chapter 2, the Microsoft security risk management process first applies a qualitative approach to identify and prioritize risks in a timely and efficient manner. However, when you select the optimal risk mitigation strategy, your estimate of the potential monetary cost of a risk is also an important consideration. Thus, for high priority or controversial risks, the process also provides guidance to determine quantitative estimates. The tasks to quantify risks occur after the detailed level risk process because of the extensive time and effort required to reach agreement on monetary estimates. You may spend considerable time quantifying low risks if you quantify risks earlier in the process.

Obviously, a monetary estimate is useful when comparing the various costs of risk mitigation strategies; however, due to the subjective nature of valuing intangible assets, no exact algorithm exists to quantify risk. The exercise of estimating an exact monetary loss can actually delay the risk assessment due to disagreements between stakeholders. The Security Risk Management Team must set expectations that the quantitative estimate is only one of many values that determine the priority or potential cost of a risk.

One benefit of using the qualitative model to prioritize risks first is the ability to leverage the qualitative descriptions to help consistently apply a quantitative algorithm. For example, the quantitative approach described below uses the asset class and exposure ratings identified in the facilitated risk discussions documented with stakeholders in the facilitated data gathering section of this chapter.

Similar to the qualitative approach, the first task of the quantitative method is to determine the total asset value. The second task is to determine the extent of damage to the asset, followed by estimating the probability of occurrence. To help reduce the degree of subjectivity in the quantitative estimate, the Microsoft security risk management process recommends using the asset classes to determine the total asset value and the exposure factor to determine the percentage of damage to the asset. This approach limits the quantitative output to three asset classes and five exposure factors, or 15 possible quantitative asset values. However, the value estimating the probability is not constrained. As appropriate for your organization, you may choose to communicate the probability in terms of a time range, or you may attempt to annualize the cost of the risk. The goal is to find a balance between the ease of selecting a relative ranking in the qualitative approach versus the difficulty of monetary valuation and estimating probability in the quantitative approach.

Use the following five tasks to determine the quantitative value:

- **Task one.** Assign a monetary value to each asset class for your organization.
- **Task two.** Input the asset value for each risk.
- **Task three.** Produce the single loss expectancy value.
- **Task four.** Determine the Annual Rate of Occurrence (ARO).
- **Task five.** Determine the Annual Loss Expectancy (ALE).

Note The tasks associated with quantifying security risks are similar to steps used in the insurance industry to estimate asset value, risk, and appropriate coverage. At the time of this writing, insurance policies for information security risks are beginning to emerge. As the insurance industry gains experience assessing information security risks, tools such as actuarial tables for information security will become valuable references in quantifying risks.

Task One: Assign Monetary Values to Asset Classes

Using the definitions for asset classes described in the facilitated data gathering section, start quantifying assets that fit the description of the high business impact class. This allows the Security Risk Management Team to focus on the most important assets to the organization first. For each asset, assign monetary values for tangible and intangible worth to the organization. For reference, use the following categories to help estimate the total impact cost for each asset:

- Replacement cost
- Sustaining/maintenance costs
- Redundancy/availability costs
- Organization/market reputation
- Organization productivity
- Annual revenue
- Competitive advantage
- Internal operating efficiencies
- Legal/compliance liability

Note The SRMGTool3-Detailed Level Risk Prioritization workbook contains a worksheet to aid in this process.

After you have monetary estimates for each category, total the values to determine the estimate for the asset. Repeat this process for all assets represented in the high business impact class. The result should be a list of priority assets and a rough estimate of their

associated monetary worth to the organization. Repeat this process for assets that fit the moderate and low business impact classes.

Within each asset class, select one monetary value to represent the worth of the asset class. A conservative approach is to select the lowest asset value in each class. This value will be used to represent an asset's worth based on the asset class selected by stakeholders during the facilitated data gathering discussions. This approach simplifies the task of assigning monetary values to each asset by leveraging the asset classes selected in the data gathering discussions.

Note Another approach for valuing assets is to work with the financial risk management team that may have insurance valuation and coverage data for specific assets.

Using Materiality for Guidance

If you are having difficulty selecting asset class values with the above method, another approach is to use the guidelines associated with the definition of materiality in financial statements produced by publicly-traded US companies. Understanding the materiality guidelines for your organization may be helpful in selecting the high asset value for the quantitative estimate.

The U.S. Financial Accounting Standards Board (FASB) documents the following regarding financial statements for publicly traded companies, "The provisions of this Statement need not be applied to immaterial items."

This passage is important to note because the FASB does not have an algorithm to determine what is material versus immaterial and warns against using strict quantitative methods. Instead, it specifically advocates considering all relevant considerations: "The FASB rejected a formulaic approach to discharging 'the onerous duty of making materiality decisions' in favor of an approach that takes into account all the relevant considerations."

While no formula exists, the US Security Exchange Commission, in [Staff Accounting Bulletin No. 99](#), acknowledges the use of a general rule of reference in public accounting to aid in determining material misstatements. For more information, see www.sec.gov/interp/account/sab99.htm. The general rule of reference cited is five percent for financial statement values. For example, one way to estimate materiality on a net income of \$8 billion would be to further analyze potential misstatements of \$400 million, or the collection of misstatements that may total \$400 million.

The materiality guidelines vary significantly by organization. Use the guidelines defining materiality as a reference only. The Microsoft security risk management process is not intended to represent the financial position of an organization in any way.

Using the materiality guidelines may be helpful for estimating the value for high business impact assets. However, materiality guidelines may not be helpful when selecting moderate and low estimates. Recognize that the exercise of estimating impact is subjective in nature. The goal is to select values that are meaningful to your organization. A good tip for determining the moderate and low values is to select a monetary value that is meaningful in relation to the amount spent on information technology in your organization. You may also choose to reference your current costs on security-specific controls to apply to each asset class. As an example, for moderate impact class assets, you can compare the value to current monetary spending on basic network infrastructure controls. For example, what is the estimated total cost for software, hardware, and operational resources in order to provide antivirus services for the organization? This provides a reference to compare assets against a known monetary amount in your organization; as another example, a moderate impact class value may be worth as much or more than the current spending on firewalls protecting assets.

Woodgrove Example The Woodgrove Security Risk Management Team worked with key stakeholders to assign monetary values to asset classes. Because risk management is new to Woodgrove, the company decided to use the materiality guidelines to form a baseline for valuing assets. It plans to revise estimates as it gains experience. Woodgrove generates an approximate net income of \$200 million annually. By applying the 5 percent materiality guideline, the HBI asset class is assigned a value of \$10 million. Based on past IT spending at Woodgrove, the stakeholders selected a value of \$5 million for MBI assets and \$1 million for LBI assets. These values were selected because large IT projects used to support and secure digital assets at Woodgrove historically have fallen into these ranges. These values will also be reevaluated during the next annual risk management cycle.

Task Two: Identify the Asset Value

After determining your organization's asset class values, identify and select the appropriate value for each risk. The asset class value should align to the asset class group selected by stakeholders in the data gathering discussions. This is the same class used in the summary and detailed level risk lists. This approach reduces the debate over a specific asset's worth, because the asset class value has already been determined. Recall that the Microsoft security risk management process attempts to strike a balance between accuracy and efficiency.

Woodgrove Example Consumer financial data was identified as HBI during the data gathering discussions; thus, the Asset Value is \$10 million based on the HBI value defined above.

Task Three: Produce the Single Loss Expectancy Value (SLE)

Next you will determine the extent of damage to the asset. Use the same exposure rating identified in the data gathering discussions to help determine the percent of damage to the asset. This percentage is called the exposure factor. The same ranking is used in the summary and detailed level risk lists. A conservative approach is to apply a linear sliding scale for each exposure rating value. The Microsoft security risk management process recommends a sliding scale of 20 percent for each exposure rating value. You may modify this as appropriate for your organization.

The last task is to multiply the asset value with the exposure factor to produce the quantitative estimate for impact. In classic quantitative models, this value is known as the single loss expectancy (SLE) value for example, asset value multiplied by the exposure factor.

For reference, the following figure provides an example of a simple quantitative approach. Note the example below simply divides the high business impact class in half to determine moderate and low values. These values may require adjustments as you gain experience in the risk assessment process.

High Business Impact Value = \$M			Exposure Rating	Exposure Factor %
			5	100
Asset Class			4	80
HBI Value	\$ M		3	60
MBI Value	\$ M/2		2	40
LBI Value	\$ M/4		1	20
Estimated Risk Value =		Asset Class Value * Exposure Factor % = SLE		

Figure 4.22: Risk Analysis Worksheet: Quantifying Single Loss Expectancy (SRMGTool3)

Woodgrove Example The following figure represents the values to determine the SLE for the two example risks.

Risk Description	Asset Class Value	Exposure Rating	Exposure Value	SLE
LAN Host Risk	\$ 10	4	80%	\$ 8
Remote Host Risk	\$ 10	4	80%	\$ 8

Figure 4.23: Woodgrove Bank SLE Example; Note Dollar Value in Millions (SRMGTool3)

Task Four: Determine the Annual Rate of Occurrence (ARO)

After you calculate single loss expectancy, you need to incorporate probability to complete the monetary risk estimate. A common approach is to estimate how often the risk may occur in the future. This estimate is then converted to an annual estimate. For example, if the Information Security Group feels that a risk may occur twice in one year, the annual rate of occurrence (ARO) is two. If a risk may occur once every three years, the ARO is one-third, 33 percent, or .33. To aid the probability estimate, use the qualitative analysis above in the detailed risk calculation. Use the following as a guide to help identify and communicate the quantitative value to determine the ARO.

Qualitative Rating	Description	ARO Range	Description Examples
High	Likely	≥ 1	Impact once or more per year
Medium	Probable	.99 to .33	At least once every 1-3 years
Low	Not probable	$< .33$	Less frequent than every 3 years

Figure 4.24: Quantifying Annual Rate of Occurrence (SRMGTool3)

Use the previous figure as a guideline only. The Information Security Group must still select one value to represent the ARO.

Woodgrove Example The Security Risk Management Team determines the following AROs for the sample risks:

- **LAN Host ARO.** Leveraging the qualitative assessment of Medium probability, the Security Risk Management Team estimates the risk to occur at least once in two years; thus, the estimated ARO is .5.
- **Remote Host ARO.** Again, leveraging the qualitative assessment of High probability, the Security Risk Management Team estimates the risk to occur at least once per year; thus, the estimated ARO is 1.

Task Five: Determine the Annual Loss Expectancy (ALE)

To complete the quantitative equation, multiply the annual rate of occurrence and the single loss expectancy. The product is represented as the annual loss expectancy (ALE).

$$\text{Annualized Loss Expectancy (ALE)} = \text{SLE} * \text{ARO}$$

The ALE attempts to represent the potential cost of the risk in annualized terms. While this may assist financially minded stakeholders in estimating costs, the Security Risk Management Team needs to reiterate the fact that impact to the organization does not fit nicely into annual expenses. If a risk is realized, the impact to the organization may occur in its entirety.

After you determine the quantitative estimate of the risk, look at the detailed risk worksheet, which contains an additional column to document any background or explanation that you want to include with the quantitative estimate. Use this column to help justify the quantitative estimate and provide supporting evidence as appropriate.

Woodgrove Example The following table shows the basic calculations to determine the ALE for each sample risk. Note how one change in any value can significantly alter the ALE value. Use the qualitative data to help justify and determine the quantitative estimate.

Risk Description	Asset Class Value	Exposure Rating	Exposure Value	SLE	ARO	Quantitative Estimate (ALE)
LAN Host Risk	\$ 10	4	80%	\$ 8	0.5	\$ 4
Remote Host Risk	\$ 10	4	80%	\$ 8	1	\$ 8

Figure 4.25: Woodgrove Bank ALE Example; Note Dollar Values in Millions (SRMGTool3)

Summary

The Assessing Risk phase of the risk management cycle is required to manage risks across the organization. When you conduct the planning, facilitated data gathering, and prioritization steps, remember that the intent of the Assessing Risk phase is not only to identify and prioritize risks, but to do so in an efficient and timely manner. The Microsoft security risk management process uses a hybrid approach of qualitative analysis to quickly identify and triage risk, then uses the financial attributes of the quantified analysis to provide further definition across risks.

Facilitating Success in the Conducting Decision Support Phase

After the Security Risk Management Team prioritizes risks to the organization, it must begin the process to identify appropriate risk mitigation strategies. To assist stakeholders in identifying possible risk mitigation solutions, the team must create functional requirements to help scope the mitigation strategy for the appropriate mitigation owner. The task of defining functional requirements is discussed within the larger decision support process in the next chapter, Chapter 5, "Conducting Decision Support."

Chapter 5: Conducting Decision Support

Overview

Your organization should now have completed the Assessing Risk phase and developed a prioritized list of risks to its most valuable assets. Now you must address the most significant risks by determining appropriate actions to mitigate them. This phase is known as Conducting Decision Support. During the previous phase, the Security Risk Management Team identified assets, threats to those assets, vulnerabilities that those threats could exploit to potentially impact assets, and the controls already established to help protect the assets. The Security Risk Management Team then created a prioritized list of risks.

The decision support process includes a formal cost-benefit analysis with defined roles and responsibilities across organizational boundaries. The cost-benefit analysis provides a consistent, comprehensive structure for identifying, scoping, and selecting the most effective and cost efficient mitigation solution to reduce risk to an acceptable level. Similar to the risk assessment process, the cost-benefit analysis requires strict role definitions in order to operate effectively. Also, before conducting the cost-benefit analysis, the Security Risk Management Team must ensure that all stakeholders, including the Executive Sponsor, have acknowledged and agreed to the process.

During the Conducting Decision Support phase, the Security Risk Management Team must determine how to address the key risks in the most effective and cost efficient manner. The end result will be clear plans to control, accept, transfer, or avoid each of the top risks identified in the risk assessment process. The six steps of the Conducting Decision Support phase are:

1. Define functional requirements.
2. Select control solutions.
3. Review solutions against the requirements.
4. Estimate the degree of risk reduction that each control provides.
5. Estimate costs of each solution.
6. Select the risk mitigation strategy.

The following figure illustrates these six steps and how the Conducting Decision Support phase relates to the overall Microsoft security risk management process.

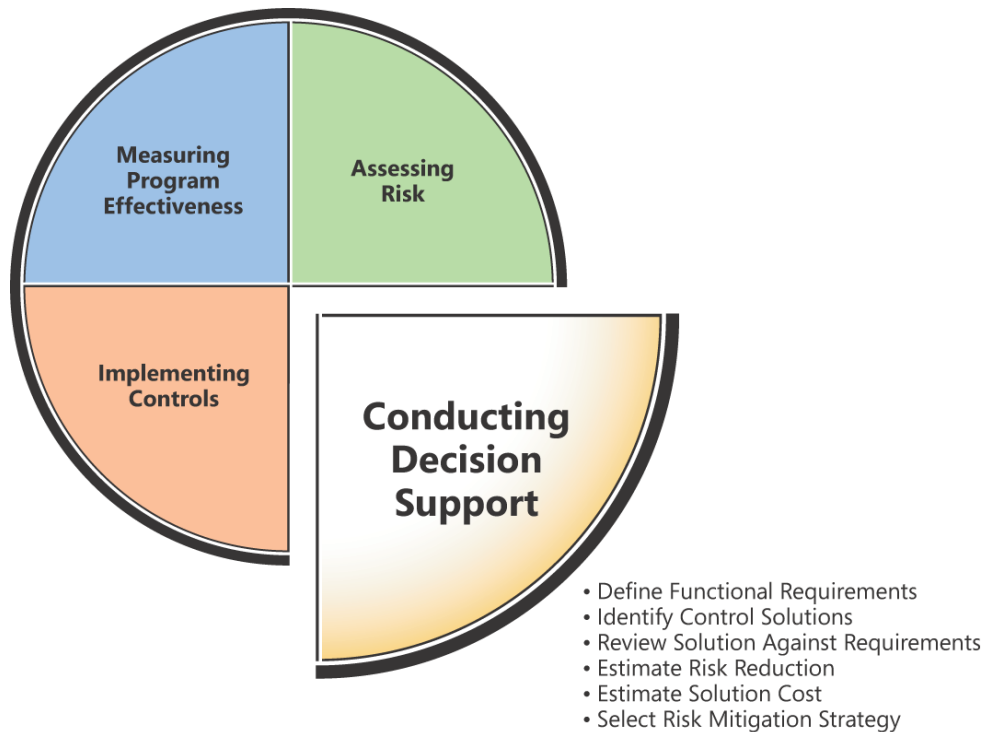


Figure 5.1: The Microsoft Security Risk Management Process: Conducting Decision Support Phase

When comparing the value of a particular control to that of another, there are no simple formulas. The process can be challenging for a variety of reasons. For example, some controls impact multiple assets. The Security Risk Management Team must agree on how to compare the values of controls that impact different combinations of assets. Additionally, there are costs associated with controls that extend beyond the implementation of those controls. Related questions to consider include:

- How long will the control be effective?
- How many person hours per year will be required to monitor and maintain the control?
- How much inconvenience will the control impose on users?
- How much training will be needed for those responsible for implementing, monitoring, and maintaining the control?
- Is the cost of the control reasonable, relative to the value of the asset?

The remainder of this chapter will discuss answers to these questions.

You will attain success during the decision support process if you follow a clear path and if participants understand their respective roles at each step. The following diagram illustrates how the Security Risk Management Team conducts the decision support process. Mitigation Owners are responsible for proposing controls that will lessen the risk and then determining the cost of each control. For each proposed control, the Security Risk Management Team estimates the degree of risk reduction that the control can be expected to provide. With these pieces of information, the team can then conduct an effective cost-benefit analysis for the control to determine whether to recommend it for implementation. The Security Steering Committee then decides which controls will be implemented.

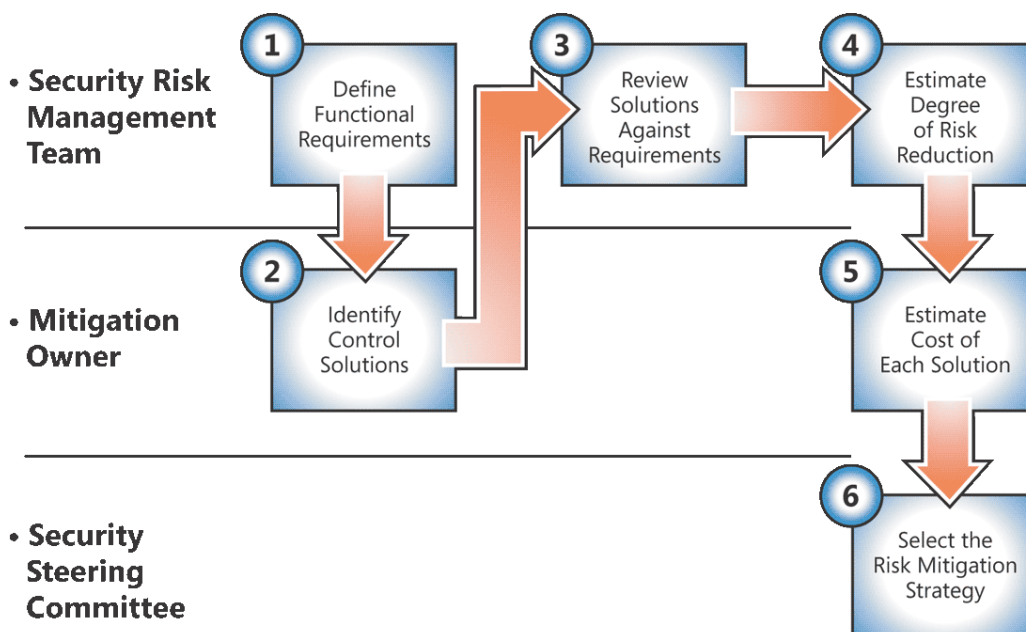


Figure 5.2: Overview of the Conducting Decision Support Phase

Clear role definitions reduce delays partly because only one group is accountable for the decision. However, experience shows that the overall effectiveness of the risk management program increases if each owner collaborates with the other stakeholders.

Note Managing risk is a perpetual cycle, so maintaining a cooperative spirit increases stakeholder morale and may actually reduce risk to the business by enabling stakeholders to recognize the benefit of their contributions and act in a timely manner to reduce risk. Obviously, you should strive to maintain and promote this attitude throughout the entire risk management and decision support processes.

Required Input for the Conducting Decision Support Phase

There is only one input from the Assessing Risk phase that is required for the Conducting Decision Support phase: the prioritized list of risks that need to be mitigated. If you followed the procedures described in Chapter 4, "Assessing Risk," then you recorded this information in the Detail Risk worksheet in the SRMGTool3-Detailed Level Risk Prioritization.xls Microsoft® Excel® workbook located in the Tools and Templates folder that was created when you unpacked the archive containing this guide and the related files. You will continue to use this same worksheet during this phase of the process.

Participants in the Conducting Decision Support Phase

Participants in the Conducting Decision Support phase are similar to those in the Assessing Risk phase; in fact, most if not all of the team members will have participated in the earlier phase. The cost-benefit analysis informs the majority of tasks in the decision support process. Before you start the cost-benefit analysis, though, be sure that all stakeholders understand their respective roles.

The following table summarizes the roles and primary responsibilities for each group in the decision support process.

Table 5.1: Roles and Responsibilities in the Risk Management Program

Role	Responsibility
Business Operations	Identifies procedural controls available to manage risk
Business Owner	Owns the cost-benefit analysis for the assets
Finance	Assists with cost-benefit analysis, may assist with budget development and control
Human Resources	Identifies personnel training requirements and controls as needed
Information Technology (IT) Architecture	Identifies and evaluates potential control solutions
IT Engineering	Determines cost of control solutions and how to implement them
IT Operations	Implements technical control solutions
Internal Audit	Identifies compliance requirements and review control effectiveness
Legal	Identifies legal, policy and contractual controls and validates value estimates created for brand impact, corporate liability, and other business issues
Public Relations	Validates value estimates created for brand impact, corporate liability, and other business issues
Security Steering Committee	Selects control solutions based on recommendations from the SRM project team
Security Risk Management Team	Defines functional requirements for the controls for each risk, communicates project status to stakeholders and affected users as needed

The Security Risk Management Team should assign a security technologist to each identified risk. A single point-of-contact reduces the risk of the Security Risk Management Team producing inconsistent messages and provides a clean engagement model throughout the cost-benefit analysis.

Tools Provided for the Conducting Decision Support Phase

Information gathered in this phase of the process should be recorded in the Detail Risk worksheet in the SRMGTool3-Detailed Level Risk Prioritization.xls Excel workbook, which is located in the Tools and Templates folder that was created when you unpacked the archive containing this guide and the related files.

Required Outputs for the Decision Support Phase

During this phase of the Microsoft security risk management process, you will define and select several key pieces of information about each of the top risks identified during the Assessing Risk phase. The following table summarizes these key elements; they are described in detail in subsequent sections of this chapter.

Table 5.2: Required Outputs for Decision Support Phase

Information to Be Gathered	Description
Decision on how to handle each risk	Whether to control, accept, transfer, or avoid each of the top risks
Functional requirements	Statements describing the functionality necessary to mitigate risk
Potential control solutions	A list of controls identified by the Mitigation Owners and the Security Risk Management Team that might be effective at mitigating each risk
Risk reduction of each control solution	Evaluation of each proposed control solution to determine how much it will reduce the level of risk to the asset
Estimated cost of each control solution	All of the costs associated with acquiring, implementing, supporting, and measuring each proposed control
List of control solutions to be implemented	Selection made through a cost-benefit analysis

Considering the Decision Support Options

Organizations have two basic tactics in terms of the way that they handle risk: They can accept a risk, or they can implement controls to reduce the risk. If they choose to accept a risk, they can then decide to transfer the risk or a portion of it to a third party such as an insurance company or a managed services company. The following two sections examine these two approaches to risk—acceptance, or implementation of controls to facilitate risk reduction.

Note Many security risk management practitioners believe that there is another option for handling each risk: avoidance. But it is important to keep in mind that when you choose to avoid a risk you decide that you will stop doing whatever activity presents the risk. With regard to security risk management, in order to avoid a risk organizations must stop using the information system that includes the risk. For example, if the risk is that "within a year, unpatched servers may become compromised via malware, which would lead to compromised integrity of financial data," the only way to avoid this risk is to stop using servers—which is probably not a realistic option. The Microsoft security risk management process assumes that organizations are only interested in examining assets that provide business value and will remain in service. Therefore, this guidance does not discuss avoidance as an option.

Accepting the Current Risk

The Security Steering Committee should choose to accept a current risk if it determines that there are no cost effective controls to productively reduce the risk. This does not mean that the organization cannot effectively address the risk by implementing one or more controls; instead, it means that the cost of implementing the control or controls, or the impact of those controls on the organization's ability to do business, is too high relative to the value of the asset needing protection. For example, consider the following scenario:

A Security Risk Management Team determines that one of the most important risks to the organization's key assets is the reliance on passwords for user authentication when logging onto the corporate network. The team identifies that deploying two-factor authentication technology such as smart cards would be the most effective way to reduce and ultimately eliminate the use of passwords for authentication. The Mitigation Owner then calculates the cost of smart card deployment throughout the organization and the

impact on the organization's existing operating systems and applications. The cost of deployment is quite high but could be justified; however, the team finds that many of the organization's internally developed business applications rely on password-based authentication and rewriting or replacing these applications would be exceedingly expensive and would take several years. Ultimately, then, for the immediate future the team decides not to recommend to the Security Steering Committee the use of smart cards for all employees. But it may in fact come to realize that a compromise would work: Users of particularly powerful or sensitive accounts such as domain administrators and key executives could be required to authenticate with smart cards. The Security Steering Committee makes the final decision to follow the recommendation of the Security Risk Management Team: Smart cards will not be required for all employees.

A variation on risk acceptance is transferal of the risk to a third party. Insurance policies for IT assets are beginning to become available. Alternatively, organizations can contract other firms that specialize in managed security services; the outsourcer may assume some or all responsibility for protecting the organization's IT assets.

Implementing Controls to Reduce Risk

Controls, sometimes described as countermeasures or safeguards, are organizational, procedural, or technological means of managing risks. The Mitigation Owners, with support from the Security Risk Management Team, identify all possible controls; calculate the cost of implementing each control; determine the other costs related to the control, such as user inconvenience or ongoing maintenance cost of the control; and assess the degree of risk reduction possible with each control. All of this information allows the team to effectively conduct a cost-benefit analysis for each proposed control. The controls that most effectively reduce risk to key assets at a reasonable cost to the organization are the controls that the team will most enthusiastically recommend for implementation.

Keys to Success

Similar to the Assessing Risk phase, setting reasonable expectations is critical if the decision support phase is to be successful. Decision support requires significant contributions from different groups representing the entire business. If even one of these groups does not understand or actively participate in the process, the effectiveness of the entire program may be compromised. Be certain to clearly explain what will be expected from each participant during the Conducting Decision Support phase, including roles, responsibilities, and degree of participation.

Building Consensus

It is important that the entire Security Risk Management Team reaches decisions by consensus whenever possible; without it, dissenting members' comments may undermine recommendations after the team presents them to the Security Steering Committee. Even if the committee endorses the recommended controls, the underlying dissension may cause the follow-up control implementation projects to fail. For the entire risk management process to succeed, all team members should agree to and support the recommended controls.

Avoiding Filibusters

Because one of the goals of this phase is to create—through consensus—a list of controls, any stakeholder involved could slow or stop progress by imposing a filibuster. That is, anyone participating in the decision support phase could decide that he or she refuses to agree to recommend a particular control. Conversely, someone could try to impose his or her minority view on the majority if a particular control's recommendation is

threatened. It is very important that the Risk Assessment Facilitator resolve filibuster situations when they arise. It is beyond the scope of this guidance to provide extensive advice on managing this type of challenge, but some effective tactics include determining the key reasons for the person's point of view and then working with the team to try to find effective alternatives or compromises that the entire team deems acceptable.

Identifying and Comparing Controls

This section explains how the Mitigation Owner will identify potential control solutions and determine the types of costs associated with implementing each proposed control, and how the Security Risk Management Team will estimate the level of risk reduction that each proposed control provides. The Mitigation Owners and Security Risk Management Team will present their findings and recommended solutions to the Security Steering Committee so that a final list of control solutions can be selected for implementation.

The following diagram is an excerpt from the Detail Risk worksheet in the Excel workbook used to perform the detailed risk assessment in the previous chapter. This worksheet, SRMGTool3-Detailed Level Risk Prioritization.xls, is included with this guide and is located in the Tools and Templates folder. The diagram shows all of the elements used during the cost-benefit analysis. Individual columns are described in the following steps.

From Prioritization process			
Quantitative impact estimate (ALE)	Quantitative description		Functional Requirement
\$ 4 Million	Estimated SLE of \$8M, ARO of .5		Implement Authentication for interactive login
\$ 8 Million	Estimated SLE of \$8M, ARO of 1.0		Implement Authentication for vpn access

Decision Support						
Functional Security Requirement	Proposed Control	Impact Rating with new control (1-10)	Probability Rating w/ New Control (1-10)	New Risk Rating (0-100)	Cost of Control Description	
Implement 2-Factor Authentication for interactive login	Smart card issuance to all users	8	1	8		
Implement 2-Factor Authentication for vpn access	Smart card issuance to all users who require remote access	8	1	8		

Figure 5.3: Decision Support Section of the Detailed Risk Worksheet (SRMGTool3)

Note The worksheet focuses on reducing the probability of impact when determining the level of risk reduction. It assumes that the value of the asset does not change within the time period of the risk assessment. Typically, the exposure level (extent of damage to the asset) remains constant. Experience shows that exposure levels usually remain unchanged if the threat and vulnerability descriptions are specified at a sufficient level of detail.

Step One: Defining Functional Requirements

Functional security requirements are statements describing the controls necessary to mitigate risk. The term "functional" is significant: Controls should be expressed in terms of the desired functions as opposed to the stated technologies. Alternative technical

solutions may be possible, and any resolution is acceptable if it meets the functional security requirement(s). The Security Risk Management Team is responsible for defining the functional requirements, the first deliverable in the cost-benefit analysis process. To properly identify potential controls, the Security Risk Management Team must define what the controls must accomplish in order to reduce risk to the business. Although the team retains ownership, collaboration with the mitigation solution owner is highly encouraged.

Functional requirements must be defined for each risk discussed in the decision support process; the deliverable produced is called "Functional Requirement Definitions." The definition and ownership of the functional requirement is very important to the cost-benefit process. The document defines what needs to occur to reduce the identified risk but does not specify how the risk should be reduced or define specific controls. This distinction gives the Security Risk Management Team responsibility in its area of expertise while also allowing the Mitigation Owner, who implements the mitigation solution, to own decisions related to running and supporting the business. Responses for each risk are documented in the column labeled "Functional Security Requirement" in SRMG3-Detailed Level Risk Prioritization.xls. Functional requirements should be reviewed at least once per year to determine whether they are still necessary or should be modified.

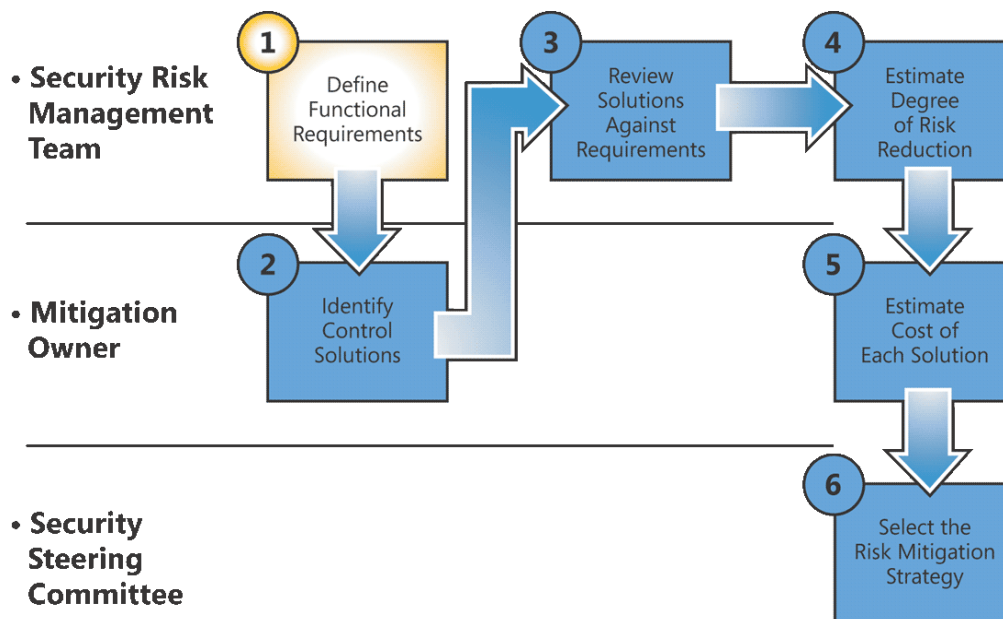


Figure 5.4: Step One of the Conducting Decision Support Phase

The work completed in the previous phase enables organizations to understand their risk positions and to rationally determine what controls should be implemented to reduce the most significant risks. The executive sponsor and business owners want to know what the Information Security Group believes the organization should do about each risk. The Information Security Group answers this by creating functional security requirements. For each risk, the Information Security Group composes a clear statement of what type of functionality or process needs to be introduced in order to mitigate the risk.

Woodgrove Example Building on the Woodgrove Bank example used in the previous chapter, a useful functional requirement for the risk of theft of credentials off a managed local area network (LAN) client via an outdated configuration of antivirus signatures, host configurations, or outdated security updates:

The ability **MUST** exist to authenticate the identity of users through two or more factors when they log on to the local network.

An example of a requirement that is not functional is:

The solution **MUST** utilize smart cards for authenticating users.

The second statement is not functional because it describes the use of a specific technology. It is up to the Mitigation Owners to provide a list specific control solutions that meet the functional requirements; it is they who translate the functional requirements into technical control solutions and/or administrative controls (policy, standards, guidelines, and so on).

The functional requirement for the second risk examined during the detailed level risk prioritization step, the risk of theft of credentials off of remote mobile hosts as a result of an outdated security configuration:

The ability **MUST** exist to authenticate the identity of users through two or more factors when they log on to the network remotely.

Record the functional requirements for each risk in the Functional Security Requirements column in SRMGTool3-Detailed Level Risk Prioritization.xls.

Internet Engineering Task Force (IETF) Request for Comments (RFC) 2119, available at www.ietf.org/rfc/rfc2119.txt, provides guidance on key words and phrases to be used in requirements statements. These terms, which are often capitalized, are "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL." Microsoft recommends that you use these key phrases in your functional requirement statements by following the definitions provided in RFC 2119:

- **MUST.** This word, or the terms "REQUIRED" or "SHALL," means that the definition is an absolute requirement of the specification. For example, if the risk assessment identifies a high risk scenario, the word "MUST" is probably the best keyword descriptor for the requirement that addresses that scenario.
- **MUST NOT.** This phrase, or the phrase "SHALL NOT," means that the definition is an absolute prohibition of the specification.
- **SHOULD.** This word, or the adjective "RECOMMENDED," means that valid reasons may exist in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. For example, if the risk assessment identifies a low risk scenario, the word "SHOULD" may be the best keyword descriptor for the requirement that addresses that scenario.
- **SHOULD NOT.** This phrase, or the phrase "NOT RECOMMENDED," means that valid reasons may exist in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- **MAY.** This word, or the adjective "OPTIONAL," means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product, while another vendor may omit the same item. An implementation that does not include a particular option **MUST** be prepared to interoperate with another implementation that does include the option, although perhaps with reduced functionality. In the same vein, an implementation that does include a particular option **MUST** be prepared to interoperate with another implementation that does not include the option (except, of course, for the feature that the option provides).

After functional requirements have been defined and documented for each risk, you are ready to move on to the next step of the Conducting Decision Support phase.

Step Two: Identifying Control Solutions

The next step in this phase is for the Mitigation Owners to come up with a list of potential new controls for each risk that address the functional requirements of that risk. For many organizations, members of the Information Security Group will be able to assist by identifying a range of potential controls for each risk that was identified and characterized

during the preceding phase. Organizations that do not have sufficient expertise in-house for this purpose can consider supplementing the Mitigation Owners with consultants.

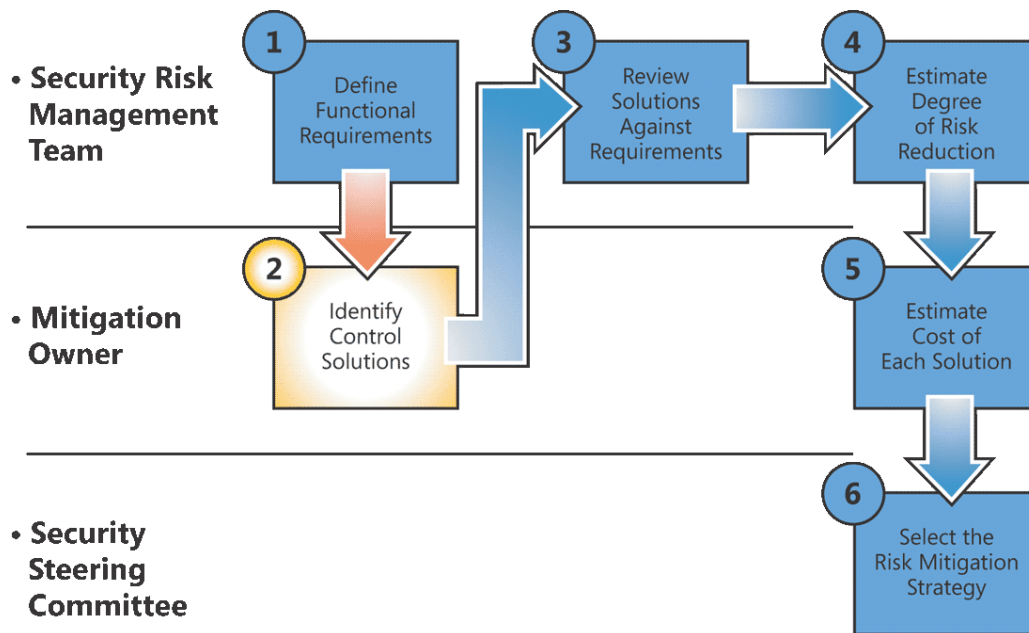


Figure 5.5: Step Two of the Conducting Decision Support Phase

The process of identifying potential controls may seem daunting, especially if few or none of the Mitigation Owners have done it before. There are two approaches that can help teams to think of new ideas; many organizations find it most effective to use both. The first is an informal brainstorming approach; the second is more organized and is based on how controls can be classified and organized. The Security Risk Management team should use a hybrid of these two approaches.

In the brainstorming approach, for each risk the Risk Assessment Facilitator poses the following series of questions to the team. The Risk Assessment Note Taker documents all responses in column labeled "Proposed Control" in the Detailed worksheet of SRMGTool3-Detailed Level Risk Prioritization.xls. This continues until all of the top risks have been examined and the team moves on to determining costs associated with each control.

- What steps could the organization undertake to resist or prevent the risk's occurrence? For example, implement multi-factor authentication to lower the risk of password compromise or deploy an automated patch management infrastructure to lower the risk of systems becoming compromised by malicious mobile code.
- What could the organization do to recover from the risk once it has taken place? For example, establish, fund, and train a robust incident response team or implement and test backup and restore processes for all computers running a server-class operating system. Going even further, an organization can establish redundant computing resources at remote locations that it can put into service should disaster strike at the primary site.
- What measures can the organization take to detect the risk occurring? For example, install a network-based intrusion detection system at the network perimeter and at key locations within the internal network, or install a distributed, host-based intrusion detection system on all computers in the organization.

- How can the control be audited and monitored to ensure that it continues to be in place? For example, install and diligently observe the appropriate management tools from the product's vendor.
- How can the organization validate the effectiveness of the control? For example, have an expert familiar with the vulnerability attempt to bypass the control.
- Are there any other actions that could be taken to manage it? For example: transfer risk by purchasing insurance to indemnify against losses relating to it.

The second method for identifying potential new controls organizes the controls into three broad categories: organizational, operational, and technological. These are further subdivided into controls that provide prevention, detection recovery, and management. Preventative controls are implemented to keep a risk from being realized, for example, they stop breaches before they transpire. Detection and recovery controls help an organization to determine when a security event has occurred and to resume normal operations afterwards. Management controls do not necessarily provide protection in and of themselves, but they are necessary for implementing other controls. These categories are discussed in more detail below.

Organizational Controls

Organizational controls are procedures and processes that define how people in the organization should perform their duties.

Preventative controls in this category include:

- **Clear roles and responsibilities.** These must be clearly defined and documented so that management and staff clearly understand who is responsible for ensuring that an appropriate level of security is implemented for the most important IT assets.
- **Separation of duties and least privileges.** When properly implemented, these ensure that people have only enough access to IT systems to effectively perform their job duties and no more.
- **Documented security plans and procedures.** These are developed to explain how controls have been implemented and how they are to be maintained.
- **Security training and ongoing awareness campaigns.** This is necessary for all members of the organization so that users and members of the IT team understand their responsibilities and how to properly utilize the computing resources while protecting the organization's data.
- **Systems and processes for provisioning and de-provisioning users.** These controls are necessary so that new members of the organization are able to become productive quickly, while leaving personnel lose access immediately upon departure. Processes for provisioning should also include employee transfers from groups within the company where privileges and access change from one level to another. For example, consider government personnel changing jobs and security classifications from Secret to Top Secret, or vice versa.
- **Established processes for granting access to contractors, vendors, partners, and customers.** This is often a variation on user provisioning, mentioned previously, but in many cases it is very distinct. Sharing some data with one group of external users while sharing a different collection of data with a different group can be challenging. Legal and regulatory requirements often impact the choices, for example when health or financial data is involved.

Detection controls in this category include:

- Performing continuing risk management programs to assess and control risks to the organization's key assets.
- Executing recurrent reviews of controls to verify the controls' efficacy.

- Periodic undertaking of system audits to ensure that systems have not been compromised or misconfigured.
- Performing background investigations of prospective candidates for employment; You should contemplate implementing additional background investigations for employees when they are being considered for promotions to positions with a significantly higher level of access to the organization's IT assets.
- Establishing a rotation of duties, which is an effective way to uncover nefarious activities by members of the IT team or users with access to sensitive information.

Management controls in this category include:

- Incident response planning, which provides an organization with the ability to quickly react to and recover from security violations while minimizing their impact and preventing the spread of the incident to other systems.
- Business continuity planning, which enables an organization to recover from catastrophic events that impact a large fraction of the IT infrastructure.

Operational Controls

Operational controls define how people in the organization should handle data, software and hardware. They also include environmental and physical protections as described below.

Preventative controls in this category include:

- Protection of computing facilities by physical means such as guards, electronic badges and locks, biometric locks, and fences.
- Physical protection for end-user systems, including devices such as mobile computer locks and alarms and encryption of files stored on mobile devices.
- Emergency backup power, which can save sensitive electrical systems from harm during power brownouts and blackouts; they can also ensure that applications and operating systems are shut down gracefully to preserve data and transactions.
- Fire protection systems such as automated fire suppression systems and fire extinguishers, which are essential tools for guarding the organization's key assets.
- Temperature and humidity control systems that extend the life of sensitive electrical equipment and help to protect the data stored on them.
- Media access control and disposal procedures to ensure that only authorized personnel have access to sensitive information and that media used for storing such data is rendered unreadable by degaussing or other methods before disposal.
- Backup systems and provisions for offsite backup storage to facilitate the restoration of lost or corrupted data. In the event of a catastrophic incident, backup media stored offsite makes it possible to store critical business data on replacement systems.

Detection and recovery controls in this category include:

- Physical security, which shields the organization from attackers attempting to gain access to its premises; examples include sensors, alarms, cameras, and motion detectors.
- Environmental security, which safeguards the organization from environmental threats such as floods and fires; examples include smoke and fire detectors, alarms, sensors, and flood detectors.

Technological Controls

Technological controls vary considerably in complexity. They include system architecture design, engineering, hardware, software, and firmware. They are all of the technological components used to build an organization's information systems.

Preventative controls in this category include:

- **Authentication.** The process of validating the credentials of a person, computer, process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital signatures, smart cards, biometric data, and a combination of user names and passwords.
- **Authorization.** The process of granting a person, computer process, or device access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access, which is verified through authentication.
- **Nonrepudiation.** The technique used to ensure that someone performing an action on a computer cannot falsely deny that he or she performed that action. Nonrepudiation provides undeniable proof that a user took a specific action such as transferring money, authorizing a purchase, or sending a message.
- **Access control.** The mechanism for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.
- **Protected communications.** These controls use encryption to protect the integrity and confidentiality of information transmitted over networks.

Detection and recovery controls in this category include:

- **Audit systems.** Make it possible to monitor and track system behavior that deviates from expected norms. They are a fundamental tool for detecting, understanding, and recovering from security breaches.
- **Antivirus programs.** Designed to detect and respond to malicious software, such as viruses and worms. Responses may include blocking user access to infected files, cleaning infected files or systems, or informing the user that an infected program was detected.
- **System integrity tools.** Make it possible for IT staff to determine whether unauthorized changes have been made to a system. For example, some system integrity tools calculate a checksum for all files present on the system's storage volumes and store the information in a database on a separate computer. Comparisons between a system's current state and its previously-known good configuration can be completed in a reliable and automated fashion with such a tool.

Management controls in this category include:

- Security administration tools included with many computer operating systems and business applications as well as security oriented hardware and software products. These tools are needed in order to effectively maintain, support, and troubleshoot security features in all of these products.
- Cryptography, which is the foundation for many other security controls. The secure creation, storage, and distribution of cryptographic keys make possible such technologies as virtual private networks (VPNs), secure user authentication, and encryption of data on various types of storage media.
- Identification, which supplies the ability to identify unique users and processes. With this capability, systems can include features such as accountability, discretionary access control, role-based access control, and mandatory access control.

- Protections inherent in the system, which are features designed into the system to provide protection of information processed or stored on that system. Safely reusing objects, supporting no-execute (NX) memory, and process separation all demonstrate system protection features.

When you consider control solutions you may also find it helpful to review the "Organizing the Control Solutions" section in Chapter 6, "Implementing Controls and Measuring Program Effectiveness." This section includes links to a variety of prescriptive guidance that was written to help organizations increase the security of their information systems.

Woodgrove Example The first risk, the risk that financial adviser user credentials could be stolen while logging on to the LAN, might be addressed by requiring users to authenticate using smart cards when connecting locally to the corporate network.

The second risk, the risk that financial adviser user credentials could be stolen while logging on to the network remotely, might be addressed by requiring all users to authenticate using smart cards when connecting remotely to the corporate network. Record each of the proposed controls for each risk in the "Proposed Control" column in SRMGTool3-Detailed Level Risk Prioritization.xls.

Step Three: Reviewing the Solution Against Requirements

The Security Risk Management Team must approve the control solution in order to ensure that the control meets the defined functional requirements. Another benefit of collaborating throughout the cost-benefit processes is the ability to anticipate the checks and balances inherent to the process, for example, if the Mitigation Owner is included in the security requirements definition, the solution will usually fit the requirements. Controls that do not meet the functional requirements for a specific risk are removed from the Detail Risk worksheet.

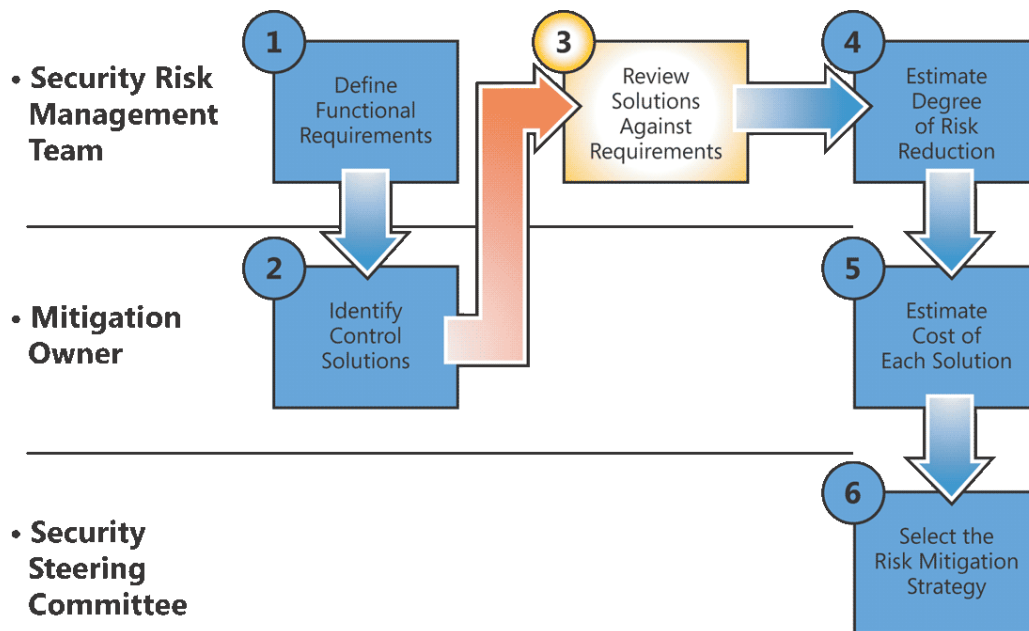


Figure 5.6: Step Three of the Conducting Decision Support Phase

Woodgrove Example The Security Risk Management Team compared the use of smart cards for user authentication to determine whether its implementation would meet the functional requirements. In this case, smart cards would indeed meet the functional requirements of both the first and second risk used in this ongoing example. Mark each of the proposed controls that are rejected by distinctively formatting them in SRMGTool3-Detailed Level Risk Prioritization.xls.

Step Four: Estimating Risk Reduction

After the Security Risk Management Team approves the potential mitigation, it must recalculate the overall risk reduction to the business. The amount of risk reduction will be compared to the cost of the mitigation solution. This is the first step in which the quantitative dollar amount may provide value in the cost-benefit analysis. Experience shows that risk reduction is usually estimated by extending the probability of the impact occurring to the business. Recall that each probability rating of high, medium, or low has a predicted time frame when the impact is likely to occur.

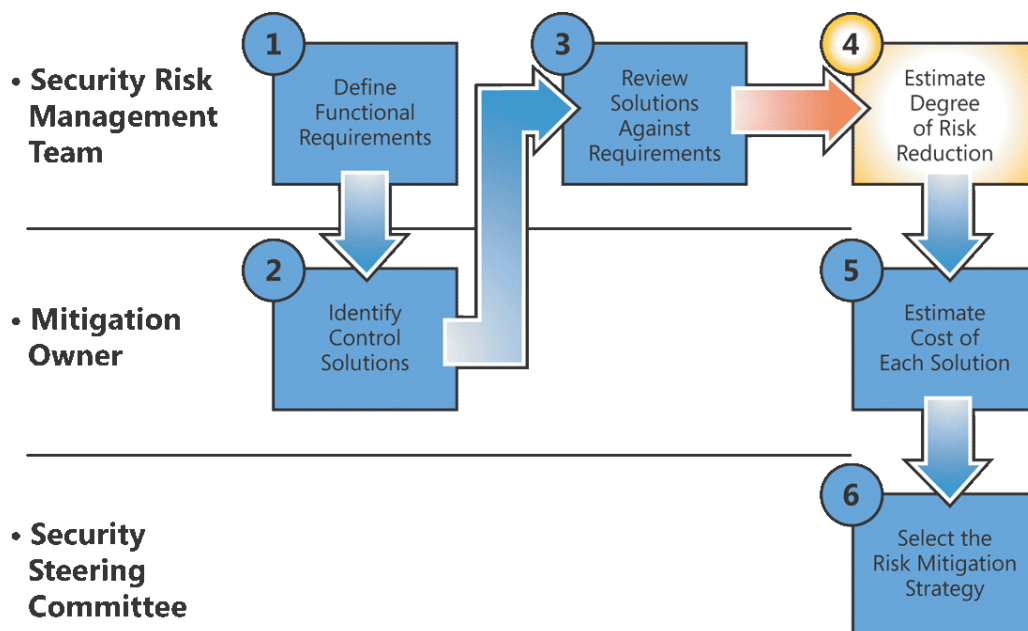


Figure 5.7: Step Four of the Conducting Decision Support Phase

Extending the estimate of when the impact may occur from one year to greater than three years provides significant value to the Security Risk Management Team and Security Steering Committee. Although the financial loss estimate may not decrease, the loss is less likely to occur in the near future. It is important to keep in mind that the goal is not to reduce the impact to zero but to define an acceptable level of risk to the business.

Another benefit of reducing the risk in the near term relates to the common trend of technical control costs decreasing over time and increasing in effectiveness. For example, an improvement in the current patch management strategy may significantly reduce the probability of host compromises today. However, the cost of deploying patches and security updates may decrease as new guidance and tools become available to effectively manage these operations. The reduction of costs using two-factor authentication provides another example of this trend.

When determining the relative degree of risk reduction for a control, be sure to consider all the ways in which the control may impact risk. Some questions to consider include:

- Does the control prevent a specific attack or a collection of attacks?
- Does it minimize the risk of a certain class of attacks?
- Does the control recognize an exploit while it is occurring?
- If it does recognize an exploit, is it then able to resist or track the attack?
- Does the control help to recover assets that have suffered an attack?

- What other benefits does it provide?
- What is the total cost of the control relative to the value of the asset?

These questions can become complex when a particular control affects multiple vulnerabilities and assets. Ultimately, the goal of this step is to make estimates for how much each control lowers the levels of risk. Record the new values for Impact Rating, Probability Rating, and Risk Rating in the columns labeled "Impact Rating with New Control," "Probability Rating with New Control," and "New Risk Rating" in SRMGTool3-Detailed Level Risk Prioritization.xls for each risk.

Woodgrove Example Regarding the first risk, the risk of financial advisers having their passwords compromised while using LAN clients, the Security Risk Management Team might conclude that the impact rating after implementing smart cards for local authentication would be 8, the probability rating would drop to 1, and the new risk rating would therefore be 8. For the second risk, the risk of financial advisers having their passwords compromised when accessing the network remotely, the Security Risk Management Team would find similar values. Record the new impact, probability, and risk ratings for each proposed control in the "Impact Rating with New Control," "Probability Rating with New Control," and "New Risk Rating" columns in the Detailed Risk worksheet of SRMGTool3-Detailed Level Risk Prioritization.xls.

Step Five: Estimating Solution Cost

The next task in this phase is for the Mitigation Owner to estimate the relative cost of each proposed control. The IT Engineering team should be able to determine how to implement each control and to provide reasonably accurate estimates on how much acquiring, implementing, and maintaining each one would cost. Because the Microsoft security risk management process entails a hybrid risk management process, precise costs do not need to be calculated; estimates should suffice. During the cost-benefit analysis, the relative values and costs of each control will be compared rather than absolute financial figures. When the team creates these estimates, it should consider all of the following direct and indirect expenditures that might be associated with a control. Record the costs for each control in the column labeled "Cost of Control Description" in SRMGTool3-Detailed Level Risk Prioritization.xls.

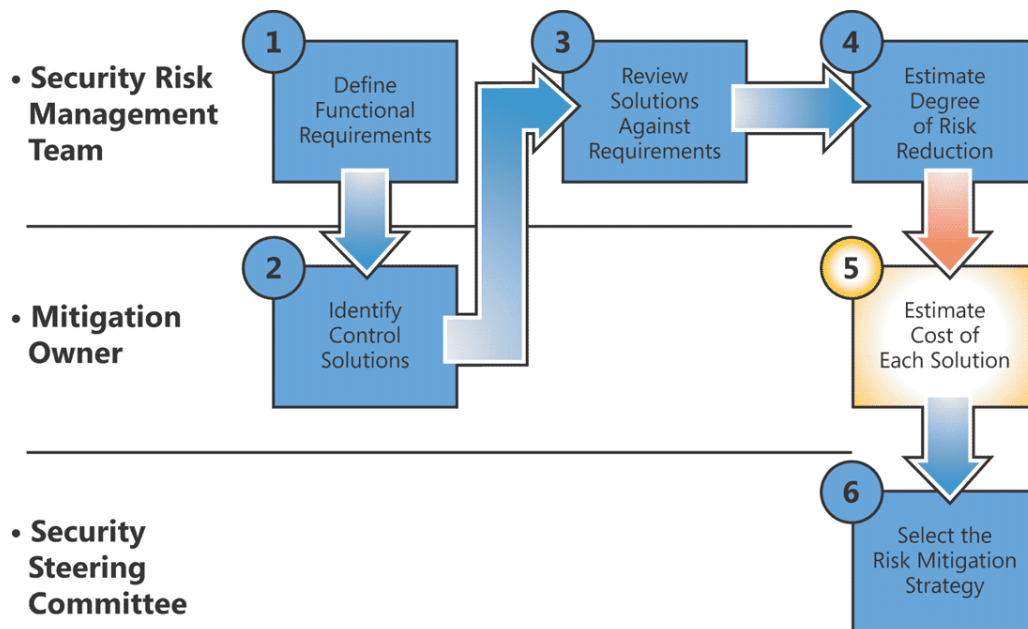


Figure 5.8: Step Five of the Conducting Decision Support Phase

Acquisition Costs

These costs comprise the software, hardware, or services related to a proposed new control. Some controls may have no acquisition costs — for example, implementing a new control may merely involve enabling a previously unused feature on a piece of network hardware that the organization is already using. Other controls may require the purchase of new technologies such as distributed firewall software or dedicated firewall hardware with application layer filtering capabilities. Some controls may not require the purchase of anything but rather the hiring of a third-party organization. For example, an organization might hire another firm to provide it with a block list of known spammers that is updated daily so that it can tie the list into its spam filters already installed on mail servers in the organization. There may be other controls that the organization chooses to develop itself; all of the costs relating to designing, developing, and testing the controls would be part of an organization's acquisition costs.

Implementation Costs

These expenditures relate to staff or consultants who will install and configure the proposed new control. Some controls may require a large team to specify, design, test, and deploy properly. Alternatively, a knowledgeable systems administrator could disable a few unused system services on all desktop and mobile computers in only a few minutes if the organization already has enterprise management tools deployed.

Ongoing Costs

These costs relate to continuing activities associated with the new control, such as management, monitoring, and maintenance. They may seem particularly hard to estimate, so try to think of them in terms of how many people will need to be involved and how much time each week (or month or year) will need to be spent on these tasks. Consider a robust, distributed network-based intrusion detection system for a large corporation with offices on four continents. Such a system would require people to monitor the system 24 hours a day, every day, and those people would have to be able to interpret and effectively respond to alerts. It might require eight or ten or even more full-time employees for the organization to fully realize the potential of this complex control.

Communication Costs

This expenditure is related to communicating new policies or procedures to users. For an organization with a few hundred employees that is installing electronic locks for its server room, a few e-mails sent to the IT staff and senior managers might be sufficient. But any organization deploying smart cards, for example, will require a lot of communication before, during, and after the distribution of smart cards and readers, because users will have to learn a whole new way of logging on to their computers and will undoubtedly encounter a wide range of new or unexpected situations.

Training Costs for IT Staff

These costs are associated with the IT staff that would need to implement, manage, monitor, and maintain the new control. Consider the previous example of an organization that has decided to deploy smart cards. Various teams within the IT organization will have different responsibilities and, therefore, require different types of training. Help desk staff will have to know how to help end users overcome common problems such as damaged cards or readers and forgotten PINs. Desktop support staff will have to know how to install, troubleshoot, diagnose, and replace the smart card readers. A team within the IT organization, one within the human resources department, or perhaps one within

the organization's physical security department will have to be responsible for provisioning new and replacement cards and retrieving cards from departing employees.

Training Costs for Users

This expenditure is related to users who would have to incorporate new behavior in order to work with the new control. In the smart card scenario referenced previously, all users will have to understand how to use the smart cards and readers, and they will also have to understand how to properly care for the cards, because most designs are more sensitive to physical extremes than credit cards or bank cards.

Costs to Productivity and Convenience

These expenditures are associated with users whose work would be impacted by the new control. In the smart card scenario, you might assume that things would be easier for an organization after the early weeks and months of deploying the cards and readers and helping users overcome their initial problems. But for most organizations, that would not be the case. Many will find that their existing applications are not compatible with smart cards, for example. In some cases this may not matter, but what about the tools that the human resources department uses to manage confidential employee information? Or the customer relationship management software used throughout the organization to track important data for all customers?

If critical business applications like these are not compatible with smart cards and are configured to require user authentication, the organization may be faced with some difficult choices. It could upgrade the software, which would require even more costs in terms of new licenses, deployment, and training. Or it could disable the authentication features, but that would lower security significantly. It could, alternatively, require users to enter user names and passwords when accessing these applications, but then users would once again have to remember passwords, undermining one of the key benefits of smart cards.

Costs for Auditing and Verifying Effectiveness

An organization would incur these expenditures after implementing the proposed new control. Examples of questions that you can ask to further define these costs include:

- How will it ensure that the control is actually doing what it was supposed to do?
- Will some members of the IT organization perform penetration testing?
- Will they try running samples of malicious code against the asset that the control is supposed to protect?
- After the effectiveness of the control has been validated, how will the organization verify that the control is still in place, on an ongoing basis?

The organization must be able to prove that nobody has accidentally or maliciously modified or disable the control, and it must determine who will be charged with the verification of this. For extremely sensitive assets it may be necessary to have more than one person validate the results.

Woodgrove Example In Tables 5.3 and 5.4, the Mitigation Owners determined costs for the risks. Record the cost estimates for each proposed control in the "Cost of Control Description" column in SRMGTool3_Detailed Level Risk Prioritization.xls.

Table 5.3: Costs for Implementing Smart Cards for VPN and Admin Access

Category	Notes	Estimates
Acquisition Costs	The cost per smart card is \$15, and the cost per reader is also \$15. Only 10,000 of the bank's employees require virtual private networking (VPN) or administrative access, so the total cost for cards and readers would be \$300,000.	\$300,000
Implementation Costs	The bank would hire a consulting firm to help it implement the solution at a cost of \$750,000. There would still be significant costs for the time invested by the bank's own employees, though: \$150,000.	\$900,000
Communication Costs	The bank already has several established methods of communicating news to employees such as printed newsletters, internal Web sites, and e-mail mailing lists, so the costs of communicating the smart card deployment would not be substantial.	\$50,000
Training Costs for IT Staff	The bank would use the same consulting organization to train the IT staff that would help with the implementation; the cost would be \$10,000. Most members of the IT staff would miss 4 to 8 hours of work time, for an estimated overall cost of \$80,000.	\$90,000
Training Costs for Users	The bank would use Web-based training from the smart card vendor for teaching employees how to use the smart cards; cost is included in the price of the hardware. Each of the bank's employees would spend about an hour taking the training, for an overall cost of lost productivity of about \$300,000.	\$300,000
Costs to Productivity and Convenience	The bank assumes that the average user will miss about an hour of productivity and that one out of four will call the Help desk for assistance with their smart cards. The cost of lost productivity would be \$300,000, and the expense of support calls to the Help desk would be \$100,000.	\$400,000
Costs for Auditing and Verifying Effectiveness	The Security Risk Management Team believes that it can periodically audit and verify the effectiveness of the new control at a cost of \$50,000 for the first year.	\$50,000
Total		\$2,090,000

Table 5.4: Costs for Implementing Smart Cards for Local Access

Category	Notes	Estimates
Acquisition Costs	The cost per smart card is \$15, and the cost per reader is also \$15. Because all 15,000 bank employees would require local access, the total cost for cards and readers would be \$450,000. The bank would also have to upgrade or replace many business applications at a substantial cost: \$1,500,000.	\$1,950,000

Implementation Costs	The bank would hire a consulting firm to help it implement the solution at a cost of \$750,000. There would still be significant costs for the time invested by the bank's own employees, though: \$150,000	\$900,000
Communication Costs	The bank already has several established methods of communicating news to employees such as printed newsletters, internal Web sites, and e-mail mailing lists, so the costs of communicating the smart card deployment would not be substantial.	\$50,000
Training Costs for IT Staff	The bank would use the same consulting organization to train the IT staff that would help with the implementation; the cost would be \$10,000. Most members of the IT staff would miss 4 to 8 hours of work time, for an estimated overall cost of \$80,000.	\$90,000
Training Costs for Users	The bank would use Web-based training from the smart card vendor for teaching employees how to use the smart cards; cost is included in the price of the hardware. Each of the bank's employees would spend about an hour taking the training, for an overall cost of lost productivity of about \$450,000.	\$450,000
Costs to Productivity and Convenience	The bank assumes that the average user will miss about an hour of productivity and that one out of four will call the Help desk for assistance with their smart cards. The cost of lost productivity would be \$450,000, and the expense of support calls to the Help desk would be \$150,000.	\$600,000
Costs for Auditing and Verifying Effectiveness	The Security Risk Management Team believes that it can periodically audit and verify the effectiveness of the new control at a cost of \$150,000 for the first year.	\$150,000
Total		\$4,190,000

Step Six: Selecting the Risk Mitigation Solution

The last step in the cost-benefit analysis is to compare the level of risk after the mitigation solution to the cost of the mitigation solution itself. Both the risk and the cost contain subjective values that are difficult to measure in exact financial terms. Use the quantitative values as a sensible test of comparison. Avoid the temptation to dismiss the intangible costs of the risk occurring. Ask the asset owner what would happen if the risk became realized. Ask the owner to document his or her response to help evaluate the importance of the mitigation solution. This tactic can be just as persuasive as an arithmetic comparison of quantitative values.

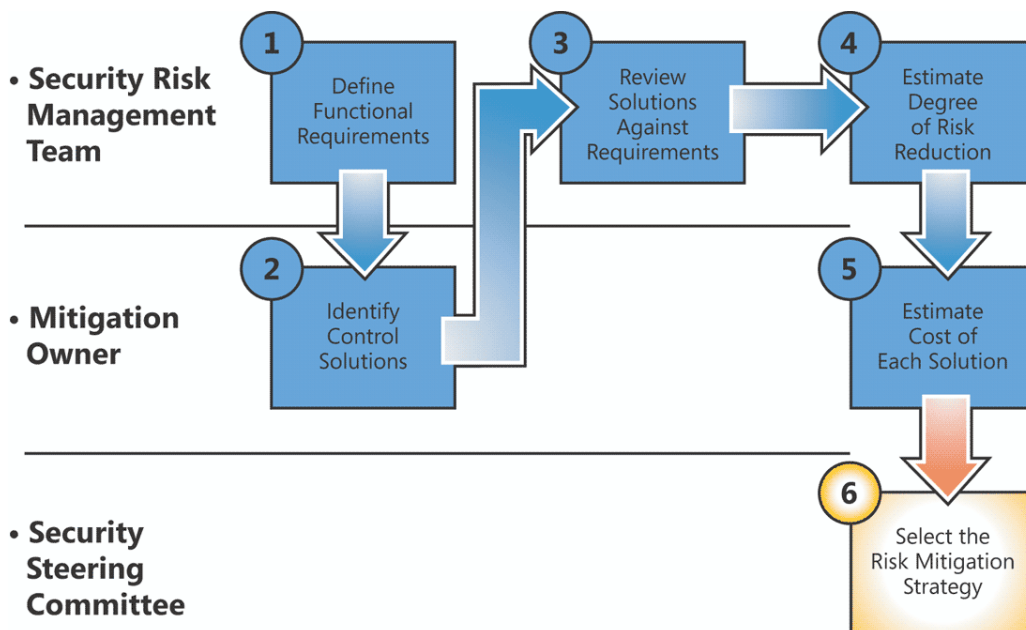


Figure 5.9: Step Six of the Conducting Decision Support Phase

A common pitfall in the cost-benefit analysis is to focus on the amount of risk reduction versus the amount of risk after the mitigation solution. This is often referred to as residual risk. As a simple example using quantitative terms, if the risk is represented as \$1000 today, and the proposed control reduces the risk by \$400, the business owner must accept the \$600 after-mitigation-solution risk. Even if the mitigation solution is less than \$400, there will still be a \$600 residual risk.

Woodgrove Example It is likely that the bank would choose to implement smart cards only for remote access, because the cost for requiring them for all user authentications is quite high. Document which of the recommended security solutions are selected for implementation before moving on to the next phase of the Microsoft security risk management process.

Summary

During the Conducting Decision Support phase, the Security Risk Management Team gathers several key pieces of additional information about each of the top risks identified during the Assessing Risk phase. For each risk, it determines whether the organization should choose to control, accept, transfer, or avoid it. The team then defines functional requirements for each risk. Next, the Mitigation Owners, coordinating with the Security Risk Management Team, create a list of potential control solutions. The team then estimates the degree of risk reduction that each control solution provides and the costs associated with each. Finally, the Security Steering Committee selects which control solutions the Mitigation Owners should implement in the next phase, Implementing Controls, which the following chapter describes.

Chapter 6: Implementing Controls and Measuring Program Effectiveness

Overview

This chapter explains the last two phases of the Microsoft security risk management process: Implementing Controls and Measuring Program Effectiveness. The Implementing Controls phase is self-explanatory: The Mitigation Owners create and execute plans based on the list of control solutions that emerged during the decision support process to mitigate the risks identified in the Assessing Risk phase. The chapter provides links to prescriptive guidance that your organization's Mitigation Owners may find helpful for addressing a variety of risks.

The Measuring Program Effectiveness phase is an ongoing one in which the Security Risk Management Team periodically verifies that the controls implemented during the preceding phase are actually providing the expected degree of protection. Another step of this phase is estimating the overall progress that the organization is making with regard to security risk management as a whole. The chapter introduces the concept of a "Security Risk Scorecard" that you can use to track how your organization is performing. Finally, the chapter explains the importance of watching for changes in the computing environment such as the addition or removal of systems and applications or the appearance of new threats and vulnerabilities. These types of changes may require the organization to take prompt action to protect itself from new or changing risks.

Implementing Controls

During this phase, the Mitigation Owners employ the controls that were specified during the previous phase. A key success factor in this phase of the Microsoft security risk management process is that the Mitigation Owners seek a holistic approach when implementing the control solutions. They should consider the entire Information Technology (IT) system, the entire business unit, or even the entire enterprise when they create their plans for acquiring and deploying mitigation solutions. The "Organizing Controls" section of this chapter provides links to prescriptive guidance that your organization may find helpful when creating plans for implementing the control solutions. This section is organized on a defense-in-depth model to make it easier for you to find guidance to address particular types of problems.

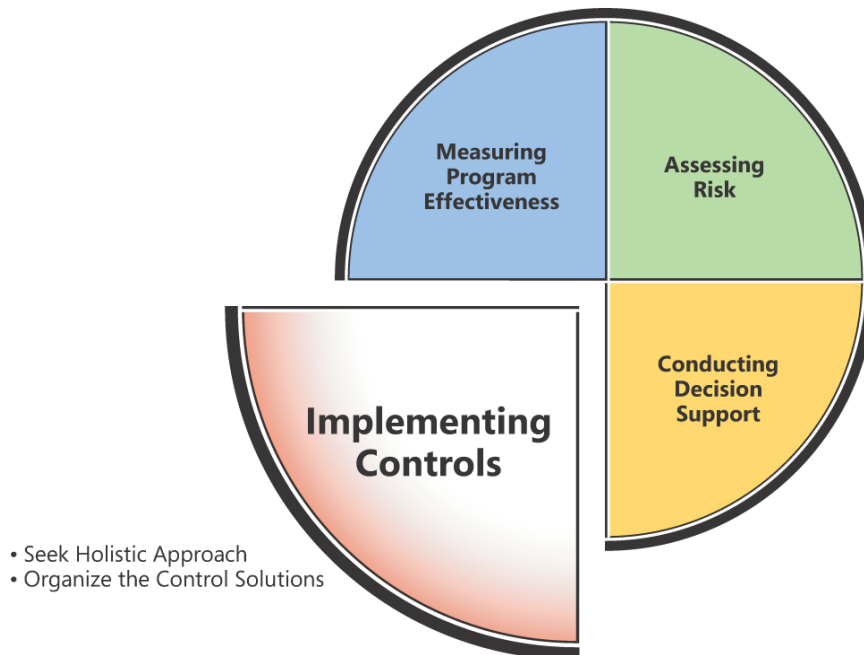


Figure 6.1: The Microsoft Security Risk Management Process: Implementing Controls Phase

Required Input for the Implementing Controls Phase

There is only one input from the Conducting Decision Support phase required for the Implementing Controls phase: the prioritized list of control solutions that need to be implemented. If you followed the procedures described in Chapter 5, "Conducting Decision Support," the Security Risk Management Team recorded this information while presenting their findings to the Security Steering Committee.

Participants in the Implementing Controls Phase

Participants in this phase are primarily the Mitigation Owners; however, they may be able to use some assistance from the Security Risk Management Team. The Implementing Controls phase includes the following roles, which were defined in Chapter 3, "Security Risk Management Overview:"

- Security Risk Management Team (Information Security Group, the Risk Assessment Facilitator, and the Risk Assessment Note Taker)
- Mitigation Owners (IT Architecture, IT Engineering, and IT Operations)

The following list summarizes specific responsibilities:

- **IT Engineering.** Determines how to implement control solutions
- **IT Architecture.** Specifies how control solutions will be implemented in a manner compatible with existing computing systems
- **IT Operations.** Implements technical control solutions

- **Information Security.** Helps to resolve issues that may arise during testing and deployment
- **Finance.** Ensures that spending levels stay within approved budgets

As a best practice, the Security Risk Management Team should assign a security technologist to each identified risk. A single point-of-contact reduces the risk of the Security Risk Management Team producing inconsistent messages and provides a clean engagement model throughout the deployment process.

Tools Provided for the Implementing Controls Phase

There are no tools included with this guide related to the Implementing Controls phase.

Required Outputs for the Implementing Controls Phase

During this phase of the Microsoft security risk management process, you will create plans to implement the control solutions specified during the Conducting Decision Support phase. The following table summarizes these key elements; subsequent sections of this chapter also summarize them.

Table 6.1: Required Outputs for the Implementing Controls Phase

Information to Be Gathered	Description
Control solutions	A list of controls selected by the Security Steering Committee and implemented by the Mitigation Owners
Reports on deployment of controls	A report or series of reports created by the Mitigation Owners describing their progress with deploying the selected control solutions

Organizing the Control Solutions

The previous chapter focused on conducting the decision support process. The result of the analysis in that phase were decisions that the Security Steering Committee related to how the organization would respond to the security risks identified during the Assessing Risk phase that preceded it. Some risks may have been accepted or transferred to third parties; for risks that were to be countered, a prioritized list of control solutions was created.

The next step is to craft action plans for implementing the controls in an explicit timeframe. These plans should be clear and precise, and each should be assigned to the appropriate person or team for execution. Use effective project management practices to track progress and ensure timely completion of project goals.

Note The Microsoft Solutions Framework (MSF) may help you successfully execute the action plans created during this phase. Designed to help organizations deliver high quality technology solutions on time and on budget, MSF is a deliberate and disciplined approach to technology projects and is based on a defined set of principles, models, disciplines, concepts, guidelines, and proven practices from Microsoft. For more information about [MSF](http://www.microsoft.com/technet/itsolutions/msf/default.aspx), see www.microsoft.com/technet/itsolutions/msf/default.aspx.

There are several critical success determinants in this phase of the project:

- The executives sponsoring the risk management project must unambiguously communicate the fact that staff members are authorized to implement the controls. Without this explicit statement in place, some employees may object to or even resist efforts to implement the new controls.
- Staff responsible for helping to implement the new controls must be allowed to reprioritize their existing duties. It must be clear to the people working on the controls and their managers that this work is a high priority initiative. If adequate resources and time are not budgeted, it is possible that the controls will not be effectively implemented. In addition, inadequate allocation of resources could lead to problems that could be unfairly attributed to the technology or control.
- The staff responsible for implementing the controls must be given adequate financial support, training, equipment, and other resources required to effectively implement each control.

The staff that implements the controls should record their progress in a report or series of reports that are subsequently submitted to the Security Risk Management Team and the Security Steering Committee.

The [Microsoft Security Center](http://www.microsoft.com/security/guidance/default.mspx), at www.microsoft.com/security/guidance/default.mspx, has an exhaustive and well-organized collection of documentation addressing a wide range of security topics. Guidance on the site may help your organization to implement selected controls from your prioritized list.

Note Much of this section is drawn from the [Microsoft Security Content Overview](http://go.microsoft.com/fwlink/?LinkId=20263) at <http://go.microsoft.com/fwlink/?LinkId=20263>. Refer to this site for the latest prescriptive security guidance from Microsoft.

The remainder of this section is organized around the Microsoft defense-in-depth model (illustrated below). Similar to publicly available models that other organizations use, the Microsoft multi-layer model organizes controls into several broad categories. The information in each section comprises recommendations of and links to prescriptive guidance and white papers describing controls for protecting every layer of a network. Prescriptive guidance provides step-by-step help for planning and deploying an end-to-end solution. This guidance has been comprehensively tested and validated in customer environments. White papers and articles generally provide good technical references for product features or pieces of an overall solution; they may not provide the breadth of information found in prescriptive guidance.

Note The "Physical Security" item in the following graphic does not have a corresponding section in this chapter recommending resources on the topic; Microsoft has not yet published detailed guidance on this subject.

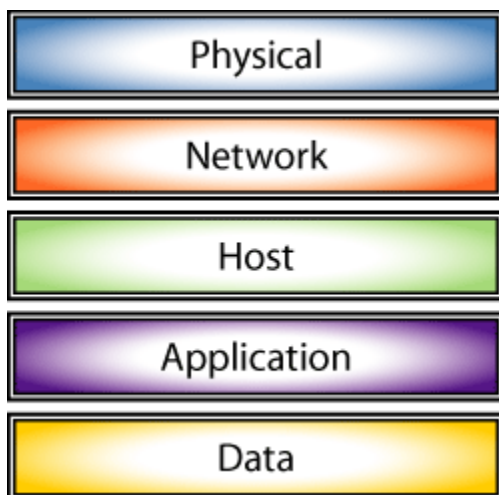


Figure 6.2: Defense-in-Depth Model

Network Defenses

A well designed and properly implemented network architecture provides highly available, secure, scalable, manageable, and reliable services. You may have multiple networks in your organization and should evaluate each individually to ensure that they are appropriately secured or that the high value networks are protected from unsecured networks. Implementing internal network defenses includes paying attention to proper network design, wireless network security, and, potentially, using Internet Protocol security (IPSec) to ensure that only trusted computers have access to critical network resources.

Prescriptive Guidance

For prescriptive guidance on securing networks with firewalls, see the "Enterprise Design for Firewalls" section of the [Firewall Services](http://www.microsoft.com/technet/itsolutions/wssra/raguide/FirewallServices/default.mspix) part of the Windows Server System Reference Architecture at www.microsoft.com/technet/itsolutions/wssra/raguide/FirewallServices/default.mspix.

For additional prescriptive guidance, see Chapter 15, "Securing Your Network," in [Improving Web Application Security: Threats and Countermeasures](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnnetsec/html/threatcounter.asp), at <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnnetsec/html/threatcounter.asp>.

For prescriptive guidance on implementing secure wireless LANs (WLANs) using EAP and digital certificates, see [Securing Wireless LANs with Certificate Services](http://go.microsoft.com/fwlink/?LinkId=14843) at <http://go.microsoft.com/fwlink/?LinkId=14843>.

For prescriptive guidance on implementing secure WLANs using PEAP and passwords, see [Securing Wireless LANs with PEAP and Passwords](http://go.microsoft.com/fwlink/?LinkId=23459) at <http://go.microsoft.com/fwlink/?LinkId=23459>.

For prescriptive guidance on using network segmentation to improve security and performance, see the "Enterprise Design" section of the [Network Architecture Blueprint](http://www.microsoft.com/technet/itsolutions/wssra/raguide/ArchitectureBlueprints/rbabna.mspix) part of the Windows Server System Reference Architecture, at <http://www.microsoft.com/technet/itsolutions/wssra/raguide/ArchitectureBlueprints/rbabna.mspix>.

White Papers and Articles

Information about IPSec deployment is available in the "Overview of IPSec Deployment" section of the [Deploying Network Services](http://technet2.microsoft.com/WindowsServer/en/Library/119050c9-7c4d-4cbf-8f38-97c45e4d01ef1033.mspix) volume of the Microsoft® Windows Server™ 2003 Deployment Kit, at <http://technet2.microsoft.com/WindowsServer/en/Library/119050c9-7c4d-4cbf-8f38-97c45e4d01ef1033.mspix>.

Additional information about using IPSec is available in the "[Using Microsoft Windows IPSec to Help Secure an Internal Corporate Network Server](http://www.microsoft.com/downloads/details.aspx?FamilyID=a774012a-ac25-4a1d-8851-b7a09e3f1dc9&DisplayLang=en)" white paper, at www.microsoft.com/downloads/details.aspx?FamilyID=a774012a-ac25-4a1d-8851-b7a09e3f1dc9&DisplayLang=en.

For a more extensive discussion of network segmentation and the issues that a solid network design can address, see the "Enterprise Design for Switches and Routers" section of the [Network Devices](http://www.microsoft.com/technet/itsolutions/techguide/wssra/raguide/Network_Devices_SB_1.mspix) part of the Windows Server System Reference Architecture, at www.microsoft.com/technet/itsolutions/techguide/wssra/raguide/Network_Devices_SB_1.mspix.

For an overview of the different types of firewalls available and how they are commonly used see "[Firewalls](http://www.microsoft.com/technet/security/topics/network/firewall.mspix)" topic at www.microsoft.com/technet/security/topics/network/firewall.mspix.

More information about network access quarantine control can be found in the following white papers:

- The "[Network Access Quarantine Control in Windows Server 2003](http://www.microsoft.com/windowsserver2003/techinfo/overview/quarantine.mspix)" white paper, at www.microsoft.com/windowsserver2003/techinfo/overview/quarantine.mspix.
- The "[Virtual Private Networking with Windows Server 2003: Overview](http://www.microsoft.com/windowsserver2003/techinfo/overview/vpnover.mspix)" white paper, at www.microsoft.com/windowsserver2003/techinfo/overview/vpnover.mspix.

Host Defenses

Hosts come in two types: clients and servers. Securing both effectively requires striking a balance between the degree of hardening and the level of usability. Although exceptions exist, the security of a computer typically increases as its usability decreases. Host defenses may include the disabling of services, removing specific user rights, keeping the operating system up to date, as well as using antivirus and distributed firewall products.

Prescriptive Guidance

The [Patch Management](http://www.microsoft.com/technet/security/topics/patch/default.mspix) Web site on Microsoft TechNet includes tools and guides to help organizations more effectively test, deploy, and support software updates. See: www.microsoft.com/technet/security/topics/patch/default.mspix.

For prescriptive guidance on securing Windows XP Professional, see the [Step-by-Step Guide to Securing Windows XP Professional with Service Pack 2 in Small and Medium Businesses](http://go.microsoft.com/fwlink/?linkid=19453) at <http://go.microsoft.com/fwlink/?linkid=19453>.

For prescriptive guidance on securing Windows XP, see the [Windows XP Security Guide](http://go.microsoft.com/fwlink/?LinkId=14839), at <http://go.microsoft.com/fwlink/?LinkId=14839>.

For prescriptive guidance on securing Windows Server 2003, see the [Windows Server 2003 Security Guide](http://go.microsoft.com/fwlink/?LinkId=14845), at <http://go.microsoft.com/fwlink/?LinkId=14845>.

The [Threats and Countermeasures Guide](http://go.microsoft.com/fwlink/?LinkId=15159) is a reference for the major security settings and features included with Windows Server 2003 and Windows XP. It provides detailed background information for use with the Windows Server 2003 Security Guide. It is available at <http://go.microsoft.com/fwlink/?LinkId=15159>.

For prescriptive guidance on securing Windows 2000 servers, see the [Windows 2000 Security Hardening Guide](http://www.microsoft.com/downloads/details.aspx?FamilyID=15E83186-A2C8-4C8F-A9D0-A0201F639A56&DisplayLang=en), at www.microsoft.com/downloads/details.aspx?FamilyID=15E83186-A2C8-4C8F-A9D0-A0201F639A56&DisplayLang=en.

White Papers and Articles

Microsoft server-class operating systems and applications use a variety of network protocols to communicate with one another and the client computers that are accessing them, including many Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports. Many of these are documented Knowledge Base (KB) article 832017, "[Service Overview and Network Port Requirements for the Windows Server System](http://support.microsoft.com/?kbid=832017)," at <http://support.microsoft.com/?kbid=832017>.

"[Antivirus Software: Frequently Asked Questions](http://www.microsoft.com/security/protect/antivirus.asp)," a brief article that provides a high-level overview of antivirus software and advice on how to acquire, install, and maintain these types of products, is available at www.microsoft.com/security/protect/antivirus.asp.

"[Internet Firewalls: Frequently Asked Questions](http://www.microsoft.com/security/protect/firewall.asp)," an article that describes the importance of using firewalls, when it is appropriate to install firewall software on user computers, and how to resolve a few of the most common problems related to using this type of software, is available at www.microsoft.com/security/protect/firewall.asp.

Application Defenses

Application defenses are essential to the security model. Applications exist within the context of the overall system, so you should consider the security of the entire environment when evaluating application security. Each application should be thoroughly tested for security compliance before running it in a production environment. The implementation of application defenses includes proper application architecture including ensuring that the application is running with the least amount of privilege with the most minimally-exposed attack surface possible.

Prescriptive Guidance

The [Exchange 2003 Hardening Guide](http://www.microsoft.com/downloads/details.aspx?FamilyID=6a80711f-e5c9-4aef-9a44-504db09b9065&displaylang=en), which provides information about securing Microsoft Exchange 2003 Server, is available at www.microsoft.com/downloads/details.aspx?FamilyID=6a80711f-e5c9-4aef-9a44-504db09b9065&displaylang=en.

The [Security Operations Guide for Exchange 2000](http://www.microsoft.com/technet/security/prodtech/mailexch/opsguide/default.mspx), which provides guidance on securing Microsoft Exchange 2000 Server, is available at www.microsoft.com/technet/security/prodtech/mailexch/opsguide/default.mspx.

The [Improving Web Application Security: Threats and Countermeasures](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/ThreatCounter.asp) solution guide, which provides a solid foundation for designing, building, and configuring secure ASP.NET Web applications, is available at <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/ThreatCounter.asp>.

Chapter 18, "[Securing Your Database Server](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/THCMCh18.asp)," of the Improving Web Application Security: Threats and Countermeasures solution guide, which includes prescriptive information about securing Microsoft SQL Server™, is available at <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/THCMCh18.asp>.

The [Building Secure ASP .NET Applications: Authentication, Authorization, and Secure Communication](http://www.microsoft.com/technet/security/prodtech/mailexch/opsguide/default.mspx) guide, which presents a practical, scenario-driven approach to designing and building secure ASP.NET applications for Windows 2000 and version 1.0 of the

Microsoft .NET Framework, is available at <http://msdn.microsoft.com/library/en-us/dnnetsec/html/secnetlpMSDN.asp?frame=true>.

White Papers and Articles

The "[Building and Configuring More Secure Web Sites](#)" white paper has detailed information about the lessons that the Microsoft security team learned during the 2002 OpenHack 4 online security contest sponsored by eWeek. The solution deployed for the contest included the .NET Framework, Microsoft Windows® 2000 Advanced Server, Internet Information Services (IIS) version 5.0, and SQL Server 2000. It successfully withstood over 82,500 attempted attacks to emerge from the competition unscathed. The paper is available at <http://msdn.microsoft.com/library/en-us/dnnetsec/html/openhack.asp>.

Data Defenses

Data is the most organizations' most valuable resource. At the client level, data is often stored locally and may be particularly vulnerable to attack. Data can be protected in a number of ways, including the use of the Encrypting File Service (EFS) and frequent, secure backups.

Prescriptive Guidance

For information about backing up data on Windows 2000–based networks, see the [Windows 2000 Server Backup and Restore Solution](#) at www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/backuprestdefault.mspx.

For step-by-step instructions on how to implement EFS, refer to the [Data Protection: Implementing the Encrypting File System in Windows 2000](#) topic, which is available at www.microsoft.com/windows2000/techinfo/planning/security/efssteps.asp.

Measuring Program Effectiveness

The Measuring Program Effectiveness phase allows the Security Risk Management Team to formally document the current state of risk to the organization. As the business continues along the risk management cycle, this phase also helps demonstrate the progress of managing risk to an acceptable level over time. To help communicate progress, this section introduces the concept of a Security Risk Scorecard as a high level indicator of risk across an organization. The scorecard helps demonstrate that risk management is truly integrated into IT operations. The concept of "integrated risk management" is also a key attribute in determining your organizations risk maturity level, as Chapter 3, "Security Risk Management Overview," described.

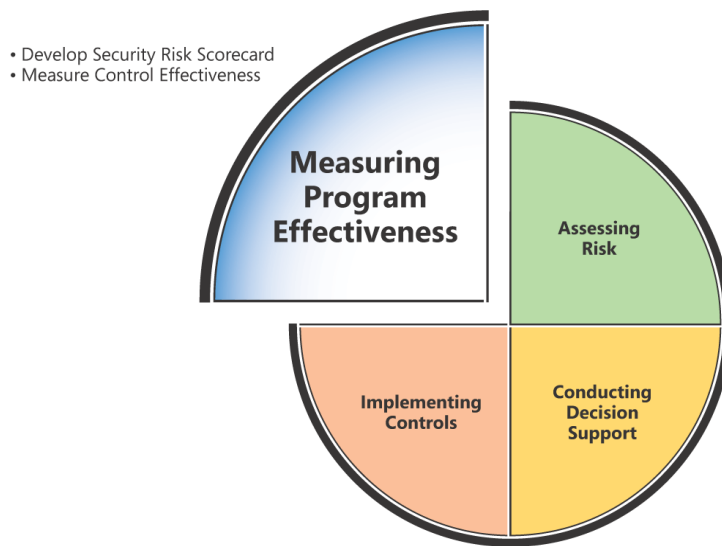


Figure 6.3: The Microsoft Security Risk Management Process: Measuring Program Effectiveness Phase

Required Inputs for the Measuring Program Effectiveness Phase

The following list summarizes the few inputs from the previous phases that are required for the Measuring Program Effectiveness phase:

- The prioritized list of risks that need to be mitigated. If you followed the procedures described in Chapter 4, "Assessing Risk," you recorded this information in the Microsoft Excel® worksheet called SRMGTool3-Detailed Level Risk Prioritization.xls, located in the Tools and Templates folder that was created when you unpacked the archive containing this guide and the related files.
- The prioritized list of control solutions that the Security Steering Committee selected. If you followed the procedures described in Chapter 5, "Conducting Decision Support," the Security Risk Management Team recorded this information while presenting its findings to the Security Steering Committee.
- Reports on deployment of controls that the Mitigation Owners created during the Implementing Controls phase that describe their progress with deploying the selected control solutions.

Participants in the Measuring Program Effectiveness Phase

The primary participants in the Measuring Program Effectiveness phase are members of the Information Security Group. They are responsible for developing the Security Risk Scorecard (explained below), verifying that the controls have been implemented and are effectively mitigating the risks as expected, and monitoring for changes to the information systems environment that may alter the organization's risk profile. The Information Security Group provides ongoing reports to the Security Steering Committee. Additionally, the Mitigation Owners assist the team by communicating major changes to the computing infrastructure and details about any security events that transpired. To

reiterate, the measuring program effectiveness process includes the following roles, which were defined in Chapter 3, "Security Risk Management Overview:"

- Security Risk Management Team (Information Security Group, the Risk Assessment Facilitator, and the Risk Assessment Note Taker)
- Mitigation Owners (IT Architecture, IT Engineering, and IT Operations)
- Security Steering Committee (Executive Sponsor, Business Owners, Architecture, and IT Engineering)

These responsibilities are summarized in the following list:

- **Information Security.** Creates summary reports for the Security Steering Committee regarding effectiveness of control solutions that have been deployed and about changes to the organization's risk profile. Additionally, creates and maintains the organization's Security Risk Scorecard.
- **Internal Audit.** Validates control solution effectiveness.
- **IT Engineering.** Communicates impending changes to the Security Risk Management Team.
- **IT Architecture.** Communicates planned changes to the Security Risk Management Team.
- **IT Operations.** Communicates details regarding security events to the Security Risk Management Team.

Tools Provided for the Measuring Program Effectiveness Phase

There are no tools included with this guide related to the Measuring Program Effectiveness phase.

Required Outputs for the Measuring Program Effectiveness Phase

During this phase, the Security Risk Management Team creates reports on the organization's ongoing security risk profile. The following table summarizes these key elements; subsequent sections of this chapter describe them in detail.

Table 6.2: Required Outputs for the Conducting Decision Support Phase

Information to Be Gathered	Description
Changes under consideration	Reports explaining changes to the information systems environment that are in the planning stage
Approved changes	Reports explaining changes to the information systems environment that are about to commence
Security events	Reports detailing unplanned security events that affected the information systems environment
Summary of control solution effectiveness	A report summarizing the degree to which the control solutions are mitigating risk

Changes to the organization's risk profile	A report showing how previously identified threats have changed due to new threats, new vulnerabilities, or changes to the organization's information systems environment
Security Risk Scorecard	A brief scorecard that illustrates the organization's current risk profile

Developing Your Organization's Security Risk Scorecard

The Security Risk Scorecard is an important tool to help communicate the current risk posture of the organization. It also helps demonstrate the progress of managing risk over time and can be an essential communication device to demonstrate the importance of risk management and its value to the organization. The scorecard should provide a summary level of risk to executive management. It is not designed to summarize the tactical view of the detailed risks identified during the Assessing Risk phase.

Note Be certain that you do not confuse the concept of the Security Risk Scorecard with IT Scorecards that are discussed in other guidance from Microsoft. Developing an IT Scorecard can be an effective way to measure an organization's progress regarding its overall information systems environment. The Security Risk Scorecard can also be valuable to that end, but it is focused on a specific part of the information systems environment: security.

The Security Risk Scorecard helps the Security Risk Management Team drive to an acceptable level of risk across the organization by highlighting problem areas and focusing future IT investments on them. Even if elements on the scorecard are ranked as High Risk, depending on your organization you may choose to accept the risk. The scorecard can then be used to help track these decisions at a high level and aids in revisiting risk decisions in future cycles of the risk management process.

The following figure represents a simple Security Risk Scorecard organized by the defense-in-depth layers as described in Chapter 4, "Assessing Risk." Customize the scorecard as needed for your organization. For example, some organizations may decide to organize risk by business units or unique IT environments. (An IT environment is a collection of IT assets that share a common business purpose and owner.) You may also want to have multiple Security Risk Scorecards if your business is quite decentralized.

	FY05 Q1	FY05 Q2	FY05 Q3	FY05 Q4
Physical	H	M		
Network	M	M		
Host	M	M		
Application	M	H		
Data	L	L		

Risk Levels (H, M, L)

Figure 6.4: Sample Security Risk Scorecard

The Security Risk Scorecard can also be part of a larger IT "dashboard" that shows key metrics across IT Operations. The practice of measuring and communicating IT metrics in a dashboard is also a best practice at Microsoft.

Measuring Control Effectiveness

After controls have been deployed, it is important to ensure that they are providing the expected protection and that they continue to remain in place. For example, it would be an unpleasant surprise to discover that the root cause of a major security breach was that the virtual private networking (VPN) authentication mechanism allowed unauthenticated users to access the corporate network because it had been misconfigured during deployment. It would be an even more unwelcome discovery that intruders had gained access to internal resources because a network engineer had reconfigured a firewall to allow additional protocols without getting prerequisite approval through the organization's change control process.

According to the U.S. Government Accountability Office's study of information security management at leading, nonfederal organizations (GAO/AIMD-98-68), direct testing was the most frequently noted method for effectively checking the degree of risk reduction achieved by controls. There are various approaches to undertaking these types of tests including automated vulnerability assessment tools, manual assessments, and penetration testing.

In a manual assessment, a member of the IT team verifies that each control is in place and appears to be functioning correctly. This can be very time consuming, tedious, and prone to error when you are checking more than a few systems. Microsoft has released a free, automated, vulnerability assessment tool called the Microsoft Baseline Security Analyzer (MBSA). MBSA can scan local and remote systems to determine which critical security hotfixes are missing, if any, as well as a variety of other important security settings. More information about [MBSA](http://www.microsoft.com/technet/security/tools/mbsahome.msp) is available at www.microsoft.com/technet/security/tools/mbsahome.msp. Although MBSA is free and very useful, other automated assessment tools are available from a variety of vendors.

The other approach mentioned previously was penetration testing, often shortened to pen testing. In a pen test, one or more people are authorized to perform automated and manual tests to see whether they can break into an organization's network in a wide

variety of ways. Some organizations perform pen tests using their own in-house security experts, while others hire outside experts who specialize in conducting these tests. Regardless of who performs the pen tests, the Information Security Group should be responsible for managing the process and tracking the results. While pen testing is an effective approach, it usually does not reveal as wide a range of vulnerabilities, because it is not as exhaustive as a properly-implemented vulnerability assessment. Therefore, it is recommended that you supplement any pen tests with other methodologies.

Note For more information about penetration testing, see the book *Assessing Network Security*, written by members of the Microsoft security team—Ben Smith, David LeBlanc, and Kevin Lam (Microsoft Press, 2004).

You can also verify compliance through other means. The Information Security Group should encourage anyone in the organization to submit feedback. Or (or additionally), the team could institute a more formal process in which each business unit is required to submit periodic compliance reports. As part of its security incident response process, the Information Security Group should create its own reports that document the symptoms that originally brought the issue to the surface, what data was exposed, what systems were compromised, and how the attack proceeded. Many things could be the cause of a security incident, including malicious code such as worms or viruses; internal users who accidentally violate policy; internal users who deliberately expose sensitive information; external attackers working for organizations such as competitors or foreign governments; and natural disasters. The steps that the Information Security Group took to contain the incident should also be documented.

The Information Security Group's effectiveness can also be tracked in several other ways, such as:

- Number of widespread security incidents that affected similar organizations but were mitigated by controls that the Security team recommended.
- Time required before computing services are fully restored after security incidents.
- Quantity and quality of user contacts.
- Number of briefings presented internally.
- Number of training classes provided internally.
- Number of assessments completed.
- Number of computer security conferences attended.
- Number and quality of public speaking engagements.
- Professional certifications achieved and maintained.

Reassessing New and Changed Assets and Security Risks

To be effective, security risk management needs to be a continuous and ongoing process within an organization rather than a temporary project. Reassessing the environment periodically by following the process described in Chapter 4, "Assessing Risk," is the first step of starting the cycle anew. It may seem obvious, but the Security Risk Management Team should reuse and update the lists of assets, vulnerabilities, controls, and other intellectual property developed during the initial risk management project.

The team can use its resources most efficiently by focusing on changes to the organization's operational environment. If there has been no change to an asset since it was last reviewed, there is no point in reviewing it in minute detail once again. The team can determine where to focus its attention by collecting timely, accurate, and relevant information about changes that impact the organization's information systems. Internal

events that should draw close scrutiny include installation of new computer software or hardware; new internally developed applications; corporate reorganizations; corporate mergers and acquisitions; and divestitures of parts of the organization. It would also be prudent to review the existing list of risks to determine whether any changes have occurred. Additionally, examining the security audit logs may provide insight on new areas to investigate.

The team should also stay alert for changes that might impact information security that take place outside of the organization. Some examples include:

- Reviewing vendor Web sites and mailing lists for new security updates and new security documentation.
- Monitoring third-party Web sites and mailing lists for information about new security research and new announcements regarding security vulnerabilities.
- Attending conferences and symposiums that include discussion of information security topics.
- Undertaking information security training.
- Staying current by reading books on computer and network security.
- Monitoring for announcements of new attack tools and methods.

Summary

During the Implementing Controls phase, the Mitigation Owners deployed the control solutions that the Security Steering Committee had chosen during the Conducting Decision Support phase. The Mitigation Owners also provided the Security Risk Management Team with reports on their progress regarding deployment of the control solutions. The fourth phase of the Microsoft security risk management process is dominated by ongoing activities that will continue to be performed until the Security Risk Management Team launches the next cycle by beginning a new security assessment. These ongoing activities include detailed reports explaining changes to the information systems environment that are in the planning stage; documenting changes to the information systems environment that are about to commence; and explaining unplanned security events that affected the information systems environment.

This phase also includes reports from the Security Risk Management Team that summarize the degree to which the control solutions are mitigating risk and a report showing how previously identified threats have changed due to new threats, new vulnerabilities, or changes to the organization's information systems environment. Finally, this phase includes creating and maintaining a Security Risk Scorecard that demonstrates the organization's current risk profile.

Conclusion to the Guide

This guide has presented the Microsoft approach to security risk management. It is a proactive approach that can assist organizations of all sizes with their response to security risks that may challenge the success of their business. A formal security risk management process enables enterprises to operate in the most cost efficient manner with a known and acceptable level of business risk and gives organizations a consistent, clear path to organize and prioritize limited resources in order to manage risk. You will realize the benefits of using security risk management when you put into place cost-effective controls that lower risk to an acceptable level.

The definition of acceptable risk, and the approach to manage risk, varies for every organization. There is no right or wrong answer; there are many risk management models in use today. Each model has tradeoffs that balance accuracy, resources, time, complexity, and subjectivity. Investing in a risk management process—with a solid framework and clearly defined roles and responsibilities—prepares the organization to articulate priorities, plan to mitigate threats, and address the next threat or vulnerability to the business.

The Microsoft security risk management process uses industry standards to deliver a hybrid of established risk management models in an iterative four-phase process that seeks to balance cost and effectiveness. During a risk assessment process, qualitative steps identify the most important risks quickly. A quantitative process follows that is based on carefully defined roles and responsibilities. This approach offers a fine degree of detail and leads to a thorough understanding of the most important risks. Together, the qualitative and quantitative steps in the risk assessment process provide the basis on which you can make solid decisions about risk and mitigation, following an intelligent business process. Now that you have read the entire guide you are ready to start the process; return to Chapter 4, "Assessing Risk," to begin.

Appendix A: Ad-Hoc Risk Assessments

The Microsoft security risk management process describes the Assessing Risk phase as a scheduled activity within the larger risk management program. The Assessing Risk phase defines the steps to identify and prioritize risk scenarios known to the organization. The result is a prioritized list of risks at both a summary level and a detail level. The scheduled risk assessment also provides the input to the remaining phases of the risk management program. While the scheduled risk assessment delivers great value, risks to the enterprise change and evolve continually as a normal part of business. Therefore, the Security Risk Management Team needs a defined process to identify and analyze risks regardless of the phase of the risk management cycle. Waiting to analyze new risks until the next scheduled round of risk assessment is not a sensible practice.

Immediate needs to understand risk may occur at any time. For example it may become apparent that there is a lack of consensus around the degree of risk surrounding a potential, or not well understood, threat. When this happens, different stakeholders may offer contradictory opinions and mitigation solutions. The Security Risk Management Team needs to document a position about the risk and help drive the decision support process, similar to the formal risk management program. It is likely that the Security Risk Management Team will be asked to create functional requirements for a given scenario that cannot and should not be derived without understanding all of the risk elements. This signals that an immediate, ad-hoc risk assessment is required. Be cautious of requests for risk assessments that attempt to misuse the risk assessment process as a means of justifying preconceived solutions or deployments. The risk assessment should result in an unbiased statement about the actual risks associated with a given issue.

In the Microsoft security risk management process, multiple risk scenarios were assessed and then prioritized. In the ad-hoc risk assessment, risks are analyzed on a case-by-case basis. An ad-hoc risk assessment focuses on a single risk issue, for example, "What are the risks associated with providing business guests wireless network access?" or "What risks are incurred by permitting mobile devices to connect to enterprise resources?" The ad-hoc risk assessment uses the methodology discussed in the process; however, prioritizing the risk and solution against other enterprise risks is not mandatory. A formal prioritization may only be necessary if the mitigation solution is costly. Often a comparison to similar risks provides sufficient perspective for the ad-hoc risk assessment to be prioritized. Of course, the ad-hoc results will be incorporated into the formal process as appropriate.

The risk discussion template included in the Tools section of this guidance can also be used for ad-hoc risk assessments. However, it is possible that data gathering may simply require research rather than a meeting with stakeholders. The Security Risk Management Team still needs to answer the key questions in the template, but the team itself may be the source of those answers. For example, if the team is trying to understand the risks associated with mobile devices, investigating the rate of device loss may be required information. This information may also be discovered by external research or through other IT teams responsible for running the service area.

The ad-hoc risk assessment can be communicated in a document structured with the following sections:

- Executive Summary. This summary should be an encapsulation of the entire assessment and should be able to be extracted from the risk assessment as a stand alone document.
- List of assumptions relating the scope and objectives of the ad-hoc risk assessment.
- A description of the asset being protected and its value to the business.
- A well-formed risk statement as described in the Microsoft security risk management process, addressing the following questions:
 - What do you want to avoid happening to the asset?
 - How might loss or exposure occur?
 - What is the extent of potential exposure to the asset?
 - What is being done today to minimize the probability of the risk occurring or minimize the impact if protective measures fail?
 - What is the overall risk? Include a statement such as "The probability is high that the attack would successfully compromise the integrity of medium-impact-value digital assets, representing high risk to the organization."
 - What are some actions that could possibly reduce the probability in the future?
 - What is the overall risk if the potential controls are implemented?

A single risk assessment may contain multiple threat scenarios. In the example of a wireless guest access solution, one scenario may be the risk of one guest attacking another guest; a second scenario may be an external attack on one of the guests; a third scenario could be a guest misusing the access to attack a target over the Internet. You should develop a risk statement for all applicable scenarios.

When the risks are understood, it may be sufficient to simply communicate them. It is also possible that the desired outcome is a statement of functional requirements from the Security Risk Management Team. If functional requirements are generated, they should be mapped to the specific risks that they address. A risk assessment document with functional security requirements is an effective tool to help the business understand risk and decide on the best mitigation solution.

Appendix B: Common Information Systems Assets

This appendix lists information system assets commonly found in organizations of various types. It is not intended to be comprehensive, and it is unlikely that this list will represent all of the assets present in your organization's unique environment. Therefore, it is important that you customize the list during the Assessing Risk phase of your project. It is provided as a reference list and a starting point to help your organization get underway.

Table B.1: Common Information Systems Assets

Asset Class	Overall IT Environment	Asset Name	Asset Rating
	<i>Highest level description of your asset</i>	<i>Next level definition (if needed)</i>	<i>Asset Value Rating, see Group definition tab (1-5)</i>
Tangible	Physical infrastructure	Data centers	5
Tangible	Physical infrastructure	Servers	3
Tangible	Physical infrastructure	Desktop computers	1
Tangible	Physical infrastructure	Mobile computers	3
Tangible	Physical infrastructure	PDA's	1
Tangible	Physical infrastructure	Cell phones	1
Tangible	Physical infrastructure	Server application software	1
Tangible	Physical infrastructure	End-user application software	1
Tangible	Physical infrastructure	Development tools	3
Tangible	Physical infrastructure	Routers	3
Tangible	Physical infrastructure	Network switches	3
Tangible	Physical infrastructure	Fax machines	1
Tangible	Physical infrastructure	PBX's	3
Tangible	Physical infrastructure	Removable media (tapes, floppy disks, CD-ROMs, DVDs, portable hard drives, PC card storage devices, USB storage devices, and so on.)	1
Tangible	Physical infrastructure	Power supplies	3

Tangible	Physical infrastructure	Uninterruptible power supplies	3
Tangible	Physical infrastructure	Fire suppression systems	3
Tangible	Physical infrastructure	Air conditioning systems	3
Tangible	Physical infrastructure	Air filtration systems	1
Tangible	Physical infrastructure	Other environmental control systems	3
Tangible	Intranet data	Source code	5
Tangible	Intranet data	Human resources data	5
Tangible	Intranet data	Financial data	5
Tangible	Intranet data	Marketing data	5
Tangible	Intranet data	Employee passwords	5
Tangible	Intranet data	Employee private cryptographic keys	5
Tangible	Intranet data	Computer system cryptographic keys	5
Tangible	Intranet data	Smart cards	5
Tangible	Intranet data	Intellectual property	5
Tangible	Intranet data	Data for regulatory requirements (GLBA, HIPAA, CA SB1386, EU Data Protection Directive, and so on.)	5
Tangible	Intranet data	U.S. Employee Social Security numbers	5
Tangible	Intranet data	Employee drivers' license numbers	5
Tangible	Intranet data	Strategic plans	3
Tangible	Intranet data	Customer consumer credit reports	5
Tangible	Intranet data	Customer medical records	5
Tangible	Intranet data	Employee biometric identifiers	5
Tangible	Intranet data	Employee business contact data	1
Tangible	Intranet data	Employee personal contact data	3
Tangible	Intranet data	Purchase order data	5
Tangible	Intranet data	Network infrastructure design	3

Tangible	Intranet data	Internal Web sites	3
Tangible	Intranet data	Employee ethnographic data	3
Tangible	Extranet data	Partner contract data	5
Tangible	Extranet data	Partner financial data	5
Tangible	Extranet data	Partner contact data	3
Tangible	Extranet data	Partner collaboration application	3
Tangible	Extranet data	Partner cryptographic keys	5
Tangible	Extranet data	Partner credit reports	3
Tangible	Extranet data	Partner purchase order data	3
Tangible	Extranet data	Supplier contract data	5
Tangible	Extranet data	Supplier financial data	5
Tangible	Extranet data	Supplier contact data	3
Tangible	Extranet data	Supplier collaboration application	3
Tangible	Extranet data	Supplier cryptographic keys	5
Tangible	Extranet data	Supplier credit reports	3
Tangible	Extranet data	Supplier purchase order data	3
Tangible	Internet data	Web site sales application	5
Tangible	Internet data	Web site marketing data	3
Tangible	Internet data	Customer credit card data	5
Tangible	Internet data	Customer contact data	3
Tangible	Internet data	Public cryptographic keys	1
Tangible	Internet data	Press releases	1
Tangible	Internet data	White papers	1
Tangible	Internet data	Product documentation	1
Tangible	Internet data	Training materials	3
Intangible	Reputation		5
Intangible	Goodwill		3
Intangible	Employee moral		3
Intangible	Employee productivity		3

IT Services	Messaging	E-mail/scheduling (for example, Microsoft Exchange)	3
IT Services	Messaging	Instant messaging	1
IT Services	Messaging	Microsoft Outlook® Web Access (OWA)	1
IT Services	Core infrastructure	Active Directory® directory service	3
IT Services	Core infrastructure	Domain Name System (DNS)	3
IT Services	Core infrastructure	Dynamic Host Configuration Protocol (DHCP)	3
IT Services	Core infrastructure	Enterprise management tools	3
IT Services	Core infrastructure	File sharing	3
IT Services	Core infrastructure	Storage	3
IT Services	Core infrastructure	Dial-up remote access	3
IT Services	Core infrastructure	Telephony	3
IT Services	Core infrastructure	Virtual Private Networking (VPN) access	3
IT Services	Core infrastructure	Microsoft Windows® Internet Naming Service (WINS)	1
IT Services	Other infrastructure	Collaboration services (for example, Microsoft SharePoint®)	

Appendix C: Common Threats

This appendix lists threats likely to affect a wide variety of organizations. The list is not comprehensive, and, because it is static, will not remain current. Therefore, it is important that you remove threats that are not relevant to your organization and add newly identified ones to it during the Assessing Risk phase of your project. It is provided as a reference list and a starting point to help your organization get underway.

Table C.1: Common Threats

Threat	Example
<i>High level description of the threat</i>	<i>Specific example</i>
Catastrophic incident	Fire
Catastrophic incident	Flood
Catastrophic incident	Earthquake
Catastrophic incident	Severe storm
Catastrophic incident	Terrorist attack
Catastrophic incident	Civil unrest/riots
Catastrophic incident	Landslide
Catastrophic incident	Avalanche
Catastrophic incident	Industrial accident
Mechanical failure	Power outage
Mechanical failure	Hardware failure
Mechanical failure	Network outage
Mechanical failure	Environmental controls failure
Mechanical failure	Construction accident
Non-malicious person	Uninformed employee
Non-malicious person	Uninformed user
Malicious person	Hacker, cracker
Malicious person	Computer criminal
Malicious person	Industrial espionage
Malicious person	Government sponsored espionage
Malicious person	Social engineering
Malicious person	Disgruntled current employee
Malicious person	Disgruntled former employee

Malicious person	Terrorist
Malicious person	Negligent employee
Malicious person	Dishonest employee (bribed or victim of blackmail)
Malicious person	Malicious mobile code

Appendix D: Vulnerabilities

This appendix lists vulnerabilities likely to affect a wide variety of organizations. The list is not comprehensive, and, because it is static, will not remain current. Therefore, it is important that you remove vulnerabilities that are not relevant to your organization and add newly identified ones to it during the Assessing Risk phase of your project. It is provided as a reference list and a starting point to help your organization get underway.

Table D.1: Vulnerabilities

Vulnerability Class	Vulnerability	Example
<i>High level vulnerability class</i>	<i>Brief description of the vulnerability</i>	<i>Specific example (if applicable)</i>
Physical	Unlocked doors	
Physical	Unguarded access to computing facilities	
Physical	Insufficient fire suppression systems	
Physical	Poorly designed buildings	
Physical	Poorly constructed buildings	
Physical	Flammable materials used in construction	
Physical	Flammable materials used in finishing	
Physical	Unlocked windows	
Physical	Walls susceptible to physical assault	
Physical	Interior walls do not completely seal the room at both the ceiling and floor	
Natural	Facility located on a fault line	
Natural	Facility located in a flood zone	
Natural	Facility located in an avalanche area	
Hardware	Missing patches	
Hardware	Outdated firmware	
Hardware	Misconfigured systems	
Hardware	Systems not physically secured	

Hardware	Management protocols allowed over public interfaces	
Software	Out of date antivirus software	
Software	Missing patches	
Software	Poorly written applications	Cross site scripting
Software	Poorly written applications	SQL injection
Software	Poorly written applications	Code weaknesses such as buffer overflows
Software	Deliberately placed weaknesses	Vendor backdoors for management or system recovery
Software	Deliberately placed weaknesses	Spyware such as keyloggers
Software	Deliberately placed weaknesses	Trojan horses
Software	Deliberately placed weaknesses	
Software	Configuration errors	Manual provisioning leading to inconsistent configurations
Software	Configuration errors	Systems not hardened
Software	Configuration errors	Systems not audited
Software	Configuration errors	Systems not monitored
Media	Electrical interference	
Communications	Unencrypted network protocols	
Communications	Connections to multiple networks	
Communications	Unnecessary protocols allowed	
Communications	No filtering between network segments	
Human	Poorly defined procedures	Insufficient incident response preparedness
Human	Poorly defined procedures	Manual provisioning
Human	Poorly defined procedures	Insufficient disaster recovery plans
Human	Poorly defined procedures	Testing on production systems
Human	Poorly defined procedures	Violations not reported
Human	Poorly defined procedures	Poor change control
Human	Stolen credentials	

Acknowledgments

The Microsoft Solutions for Security and Compliance group (MSSC) and the Microsoft Security Center of Excellence (SCOE) would like to acknowledge and thank the team that produced The Security Risk Management Guide. The following people were either directly responsible or made a substantial contribution to the writing, development, and testing of this solution.

Authors

Kurt Dillard
Jared Pfost
Stephen Ryan, Content Master

Content Contributors

Price Oden
Jeff Williams

Testers

Dan Hitchcock
Mehul Mediwala, Infosys Technologies
Pete Narmita
Price Oden
Jason Wong

Editors

Wendy Cleary, S&T Onsite
Jennifer Kerns, Content Master

Release Managers

Flicka Crandell
Karl Seng, Siemens

Program Managers

Karl Grunwald
Alison Woolford, Content Master

Contributors

Chase Carpenter
Brian Fielder
Michael Glass, Volt
John Howie
Maxim Kapteijns
Chrissy Lewis, Siemens
Keith Proctor
Bill Reid
Lee Walker

Reviewers

Shanti Balaraman
Rich Bennack, US GTSC Security
Mathieu Groleau
Alan Hakimi
Ellen McDermott
Marco Nuijen
Brian Shea, Bank of America
David Smith
Brad Warrender
John Weigelt
Jessica Zahn

At the request of Microsoft, the United States Department of Commerce National Institute of Standards and Technology (NIST) also participated in the review of these Microsoft documents and provided comments, which were incorporated into the published versions.