# Complete Report

This report contains the following sections:

* [Executive Summary](#ExecSum)
  + [Introduction](#Introduction)
  + [Background: Assessment Process and Scope](#AssessmentProcessScope)
  + [Situation Analysis](#SituationAnalysis)
  + [Scorecard](#Scorecard)
  + [Security Initiatives](#SecurityInitiatives)
* [Assessment in Detail](#AssessmentInDetial)
  + [Areas of Analysis](#AreasOfAnalysis)
  + [Assessment Analysis](#AssessmentAnalysis)
    - [Infrastructure](#Infrastructure)
    - [Applications](#Applications)
    - [Operations](#Operations)
    - [People](#People)
* [Prioritized Action List](#PrioritizedActionList)
* [Appendices](#Appendices)
  + [Questions and Answers](#QuestionsAnswers)
  + [Glossary](#Glossary)
  + [Interpreting the Graphs](#InterpretingTheGraphs)

A Microsoft partner can review this report with you and help with developing a detailed action plan for implementing the recommendations. If you do not have an existing relationship with a Microsoft partner, you may wish to view a list of Microsoft Partners for Security Solutions at <https://solutionfinder.microsoft.com/>.

The Microsoft Security Assessment Tool is designed to help you determine the level of risk your computing infrastructure faces and the steps you have taken to mitigate that risk, and to offer suggestions of additional steps you can take to help further reduce your level of risk. It is not a replacement for an audit by a professional security consultant.  
Use of the Microsoft Security Assessment Tool is governed by the terms of the End-User License Agreement (EULA) which accompanied the software, and this report is subject to the exclusions, disclaimers, and limitations of liability contained in the EULA.  
  
This report is for informational purposes only. Neither Microsoft Corporation, its suppliers, or partners make any representation or warranty of any kind, whether express or implied, concerning the Security Assessment Tool, or the use, accuracy, or reliability of the results of the Assessment and information contained in this report.

## Executive Summary

### ****Introduction****

**This Microsoft Security Assessment Tool is designed to assist you with identifying and addressing security risks in your computing environment. The tool employs a holistic approach to measuring security strategy by covering topics across people, process, and technology. Findings are coupled with recommended mitigation efforts, including links to more information for additional guidance if needed. These resources may assist you in learning more about the specific tools and methods that can help increase the security of your environment.**

**This summary section is intended to give IT and senior managers a snapshot of the company's overall security posture. Detailed findings and recommendations can be found in the detailed report following.**

### ****Background: Assessment Process and Scope****

**The assessment is designed to identify the business risk of your organization and the security measures deployed to mitigate risk. Focusing on common issues in this market segment, the questions have been developed to provide a high-level security risk assessment of the technology, processes, and people that support the business.**

**Beginning with a series of questions about your company's business model, the tool builds a Business Risk Profile (BRP), measuring the risk of doing business your company must face due to the industry and business model chosen. A second series of questions are posed to compile a listing of the security measures your company has deployed over time. Together, these security measures form layers of defense, providing greater protection against security risk and specific vulnerabilities. Each layer contributes to a combined strategy for defense-in-depth. This sum is referred to as the Defense-in-Depth Index (DiDI). The BRP and DiDI are then compared to measure risk distribution across the areas of analysis (AoAs)—infrastructure, applications, operations, and people.**

**In addition to measuring the alignment of security risk and defenses, this tool also measures the security maturity of your organization. Security maturity refers to the evolution of strong security and maintainable practices. At the low end, few security defenses are employed and actions are reactive. At the high end, established and proven processes allow a company to be more proactive, and respond more efficiently and consistently when needed.**

**Risk management recommendations are suggested for your environment by taking into consideration existing technology deployment, current security posture, and defense-in-depth strategies. Suggestions are designed to move you along a path toward recognized best practices.**

**This assessment—including the questions, measures, and recommendations—is designed for midsize organizations that have between 50 and 500 desktops in their environment. It is meant to broadly cover areas of potential risk across your environment, rather than provide an in-depth analysis of a particular technology or process. As a result, the tool cannot measure the effectiveness of the security measures employed. To that end, this report should be used as a preliminary guide to help you focus on specific areas that require more rigorous attention, and should not replace a focused assessment by trained third-party assessment teams.**

### ****Situation Analysis****

**This section graphically represents the concepts described above for your organization, based on the answers you provided. As a reminder:**

* **BRP is a measure of the risk related to the industry and business model of the company**
* **DiDI is a measure of the security defenses used across people, process, and technology to help mitigate identified risks to the business**
* **Security Maturity is a measure of the organization's ability to effectively use the tools available to create a maintainable security level across many disciplines**

**[See** [Appendices](#Appendices) **for additional information on these terms and how to interpret the graphs.]**

### ****Results:****

|  |  |  |
| --- | --- | --- |
| ****Areas of Analysis**** | Risk-Defense Distribution | Security Maturity |
| **Infrastructure** | **** | **** |
| **Applications** | **** | **** |
| **Operations** | **** | **** |
| **People** | **** | **** |

### ****Risk-Defense Distribution****

**This chart indicates differences in the Defense-in-Depth score, organized by Area of Analysis.**

**In general, it is best to have a DiDI rating on par with the BRP rating for the same category. An imbalance either within a category or across categories—in either direction—may indicate the need to realign your IT investments.**

### ****Security Maturity****

Security maturity is inclusive of controls (both physical and technical), the technical acumen of IT resources, policy, process, and maintainable practices. Security maturity can be measured only through the organization's ability to effectively use the tools available to create a maintainable security level across many disciplines. A baseline of security maturity should be established and used to define areas of focus for the organization's security programs. Not all organizations should strive to reach the optimized level, but all should assess where they are and determine where they should be, in light of the business risk they face. For example, a company with a low-risk environment may never need to advance beyond the upper range of the Baseline level or the lower range of the Standardized level. A company with a high-risk environment will likely push well into the Optimized level. Your Business Risk Profile scores help you gauge your risk.

|  |  |
| --- | --- |
| **Security Maturity** | A measure of a company's practices against industry best practices for maintainable security. Each company should strive to align its maturity level, and associated security strategy, relative to the risks taken in doing business: |
|  |
| **Baseline** | Some proactive security measures deployed as first-line defenses; operations and incident response still very reactive |
|  |
| **Standardized** | Multiple layers of defense deployed in support of a defined strategy |
|  |
| **Optimized** | Effectively protecting the right things the right way and ensuring ongoing utilization of best practices |
|  |

### Scorecard

Based on your answers to the risk assessment, the following ratings have been applied to your defensive measures. The [Assessment Detail](#AssessmentInDetial) and [Prioritized Action List](#PrioritizedActionList) sections of this report include further detail for each, including the findings, best practices, and recommendations.

|  |  |  |  |
| --- | --- | --- | --- |
| Legend: | Meets best practice | Needs improvement | Severely lacking |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Infrastructure** |  | | **Perimeter Defense** |  | | Firewall Rules and Filters |  | | Anti-virus |  | | Anti-virus - Desktops |  | | Anti-virus - Servers |  | | Remote Access |  | | Segmentation |  | | Intrusion-Detection System (IDS) |  | | Wireless |  | | **Authentication** |  | | Administrative Users |  | | Internal Users |  | | Remote-Access Users |  | | Password Policies |  | | Password Policies - Administrator Account |  | | Password Policies - User Account |  | | Password Policies - Remote-Access Account |  | | Inactive Accounts |  | | **Management and Monitoring** |  | | Incident Reporting & Response |  | | Secure Build |  | | Physical Security |  | | **Applications** |  | | **Deployment and Use** |  | | Load-Balancing |  | | Clustering |  | | Application & Data Recovery |  | | Third-party independent software vendor (ISV) |  | | Internally Developed |  | | Vulnerabilities |  | | **Application Design** |  | | Authentication |  | | Password Policies |  | | Authorization & Access Control |  | | Logging |  | | Input Validation |  | | Software Security Development Methodologies |  | | **Data Storage & Communications** |  | | Encryption |  | | Encryption - Algorithm |  | | |  |  | | --- | --- | | **Operations** |  | | **Environment** |  | | Management Host |  | | Management Host - Servers |  | | Management Host - Network Devices |  | | **Security Policy** |  | | Data Classification |  | | Data Disposal |  | | Protocols & Services |  | | Acceptable Use |  | | User Account Management |  | | Governance |  | | Security Policies |  | | **Patch & Update Management** |  | | Network Documentation |  | | Application Data Flow |  | | Patch Management |  | | Change Management and Configuration |  | | **Backup and Recovery** |  | | Log Files |  | | Disaster Recovery & Business Resumption Planning |  | | Backup |  | | Backup Media |  | | Backup & Restore |  | | **People** |  | | **Requirements & Assessments** |  | | Security Requirements |  | | Security Assessments |  | | **Policy & Procedures** |  | | Background Checks |  | | Human Resources Policy |  | | Third-Party Relationships |  | | **Training & Awareness** |  | | Security Awareness |  | | Security Training |  | |

### Security Initiatives

The following areas fall short of best practices and should be addressed to increase the security of your environment. The [Assessment Detail](#AssessmentInDetial) and [Prioritized Action List](#PrioritizedActionList) sections of this report include further detail for each, including the findings, best practices, and recommendations.

|  |  |  |
| --- | --- | --- |
| High Priority | Medium Priority | Low Priority |
| * Third-Party Relationships * Vulnerabilities * Security Assessments * Security Requirements * Application & Data Recovery | * Security Awareness * Encryption * Encryption - Algorithm * Administrative Users * Software Security Development Methodologies | * Management Host - Servers * Management Host - Network Devices * Backup * Anti-virus - Desktops * Anti-virus - Servers |

**Assessment in Detail**

This section of the report provides the detailed findings for each category, as well as best practices, recommendations, and references for additional information. Recommendations are prioritized in the following section.

### Areas of Analysis

**The following table lists the areas that were included for high-level analysis in this security risk assessment and describes each area's relevance to security. The Assessment Detail section of this document describes your organization's security posture (based on answers you gave during the assessment) in each of these areas and provides industry-recognized best practices and recommendations for achieving those practices.**

|  |  |
| --- | --- |
| **Category** | **Importance to security** |
| **Business Risk Profile** | |
| Business Risk Profile | Understanding how the nature of your business affects risk is important in determining where to apply resources in order to help mitigate those risks. Recognizing critical areas of business risk will help you to optimize allocation of your security budget. |
| **Infrastructure** | |
| Perimeter Defense | Perimeter defense addresses security at network borders, where your internal network connects to the outside world. This constitutes your first line of defense against intruders. |
| Authentication | Rigorous authentication procedures for users, administrators, and remote users help to ensure that outsiders do not gain unauthorized access to the network through the use of local or remote attacks. |
| Management & Monitoring | Management, monitoring, and proper logging are critical to maintaining and analyzing IT environments. These tools are even more important after an attack has occurred and incident analysis is required. |
| **Applications** | |
| Deployment & Use | When business-critical applications are deployed in production, the security and availability of those applications and servers must be ensured. Continued maintenance is essential to help ensure that security bugs are patched and that new vulnerabilities are not introduced into the environment. |
| Application Design | Design that does not properly address security mechanisms such as authentication, authorization, and data validation can allow attackers to exploit security vulnerabilities and thereby gain access to sensitive information. |
| Data Storage & Communications | Integrity and confidentiality of data is one of the greatest concerns for any business. Data loss or theft can hurt an organization's revenue as well as reputation. It is important to understand how applications handle business critical data and how that data is protected. |
| **Operations** | |
| Environment | The security of an organization is dependent on the operational procedures, processes and guidelines that are applied to the environment. They can enhance the security of an organization by including more than just technology defenses. Accurate environment documentation and guidelines are critical to the operation team's ability to support and maintain the security of the environment. |
| Security Policy | Corporate security policy refers to individual policies and guidelines that exist to govern the secure and appropriate use of technology and processes within the organization. This area covers policies to address all types of security, such as user, system, and data. |
| Patch & Update Management | Good management of patches and updates is important to securing an organization's IT environment. The timely application of patches and updates is necessary to help protect against known and exploitable vulnerabilities. |
| Backup and Recovery | Data backup and recovery is essential to maintaining business continuity in the event of a disaster or hardware/software failure. Lack of appropriate backup and recovery procedures could lead to significant loss of data and productivity. |
| **People** | |
| Requirements & Assessments | Security requirements should be understood by all decision-makers so that both their technical and business decisions enhance security rather than conflict with it. Regular assessments by a third party can help a company review, evaluate, and identify areas for improvement. |
| Policies and Procedures | Clear, practical procedures for managing relationships with vendors and partners can help limit your company's exposure to risk. Procedures covering employee hiring and termination can help protect your company from unscrupulous or disgruntled employees. |
| Training & Awareness | Employees should be trained and made aware of how security applies to their daily job activities so that they do not inadvertently expose their company to greater risks. |

### Assessment Analysis

This section is divided into the four major areas of analysis—Infrastructure, Applications, Operations, and People.

### Infrastructure

Infrastructure security focuses on how the network should function, what business processes (internal or external) it must support, how hosts are built and deployed, and how the network will be managed and maintained. Effective infrastructure security can help provide significant improvements in the areas of network defense, incident response, network availability, and fault analysis. By establishing a sound infrastructure design that is understood and followed, an organization can identify areas of risk and can design methods of threat mitigation. The assessment reviews high-level procedures that an organization can follow to help mitigate infrastructure risk by focusing on the following areas of infrastructure security:

* Perimeter Defense — Firewalls, Anti-virus, Remote Access, Segmentation, Intrusion Detection Systems, Wireless Security
* Authentication — Administrative, Internal & Remote Users, Password Policies, Inactive Accounts
* Management & Monitoring — Incident Reporting & Response, Secure Build, Physical Security

|  |  |  |
| --- | --- | --- |
| **Perimeter Defense** | | |
| **Subcategory** | **Best Practices** | |
| **Firewall Rules and Filters** | Firewalls are a first-line defense mechanism and should be placed at all network border locations. Rules implemented on firewalls should be highly restrictive and set on a host-by-host and service-by-service basis. When creating firewall rules and router ACLs (Access Control Lists), focus on first protecting access control devices and the network from attack.    + Enforce data flow by use of network ACLs and firewall rules.  + Test firewall rules and router ACLs to determine whether or not existing rules contribute to Denial of Service (DoS) attacks. + Deploy one or more DMZs as part of a systematic and formal firewall development.  + Place all Internet accessible servers there. Restrict connectivity to and from the DMZs. | |
|  | **Findings** | **Recommendations** |
| **Firewall Rules and Filters** | You have indicated that firewalls are deployed at each office location. | Continue deploying firewalls or other network-level access controls at each office location, and frequently test and verify that all firewalls are working properly. |
| **Firewall Rules and Filters** | You have indicated that host-based firewall software is used to protect servers. | Continue installing host-based firewalls on all servers, and consider extending this software to all desktops and laptops in the organization also. |
| **Firewall Rules and Filters** | You have indicated that the firewall is tested regularly to ensure proper performance. | Continue regular testing of your firewall. Ensure that functionality is working as expected not only from external traffic, but that the firewall is also behaving as expected towards internal traffic. |
| **Firewall Rules and Filters** | Your answers indicate that while you have taken the first step in perimeter defense by deploying a firewall at network border locations, you have not created a DMZ segment to protect Internet-accessible corporate resources from internal corporate resources. | Consider deploying a firewall to separate Internet-accessible resources, such as Web servers, from internal corporate resources. Implement rules for controlling inbound and outbound access. Consider implementing egress filtering to prevent unnecessary outbound connections and limit direct access to DMZ segments by internal users, as it is not likely users would work on a regular basis with the host computers that reside in the DMZ.  Limit access from the core network into the DMZ segment to only specific hosts or administrative networks. |
| **Subcategory** | **Best Practices** | |
| **Anti-virus** | Deploy anti-virus solutions throughout the environment on both the server and desktop levels. Deploy specialized anti-virus solutions for specific tasks such as file server scanners, content screening tools, and data upload and download scanners. Configure anti-virus solutions to scan for viruses both entering and leaving the environment. Anti-virus solutions should be implemented first on critical file servers and then extended to mail, database, and Web servers.  For desktops and laptops an anti-virus solution should be included in the default build environment.  If you are using Microsoft Exchange, use the additional anti-virus and content filtering-capabilities it offers at the mailbox level. | |
| **Subcategory** | **Best Practices** | |
| **Anti-virus - Desktops** |  | |
|  | **Findings** | **Recommendations** |
| **Anti-virus - Desktops** | Your answer indicates that anti-virus solutions have been deployed at the desktop level. | Continue the practice. Implement a policy that requires users to regularly update virus signatures. Consider adding the anti-virus client in the default workstation build environment. |
| **Subcategory** | **Best Practices** | |
| **Anti-virus - Servers** |  | |
|  | **Findings** | **Recommendations** |
| **Anti-virus - Servers** | Your answer indicates that you have deployed anti-virus solutions at the server level. | Continue the practice. Consider actively managing anti-virus clients on the servers from a centralized management console for configuration and signature deployment. If you are using Microsoft Exchange, consider using the additional anti-virus and content filtering capabilities at the mailbox level. |
| **Subcategory** | **Best Practices** | |
| **Remote Access** | Workstations are a critical factor in the defense of any environment, especially if there are remote and roaming users that connect to the environment. Tools such as personal firewalls, anti-virus, and remote-access software should be present and properly configured on all workstations.   Implement a policy which requires periodic review of these tools to make sure their configurations reflect changes in applications and services being used, but at the same time still keep the workstation resistant to attacks. | |
|  | **Findings** | **Recommendations** |
| **Remote Access** | Your answers indicate that not only have you implemented a VPN for remote access, but you have also incorporated multifactor authentication as a second line of defense. | Regularly audit the access list for all the users on the VPN device. Consider managing the VPN device from inside the corporate network only. |
| **Subcategory** | **Best Practices** | |
| **Segmentation** | Use segmentation to separate specific extranets from vendor, partner, and customer access. Each external network segment should allow only specific application traffic to be routed to the specific application hosts and ports that are used to supply services to customers.  Ensure that network controls are in place to restrict access to only what is required for each third-party connection.  Restrict access to and from the network services being provided, and restrict access between network segments. | |
|  | **Findings** | **Recommendations** |
| **Segmentation** | Your response indicates that Internet-facing services are not hosted on your organization's network | If Internet facing services are going to be hosted on the company's network, ensure that firewalls, segmentation and intrusion-detection systems are in place in order to protect the company's infrastructure from Internet-based attacks. |
| **Segmentation** | You have indicated that the network only has one segment. | Use segmentation to separate specific extranets and vendor, partner, or customer access. Each external network segment should only allow specific application traffic to be routed to specific application hosts and ports used to supply services to customers.  Ensure that network controls are in place to restrict access to only what is required for each third-party connection.  Restrict access to and from the network services being provided and restrict access between network segments. |
| **Subcategory** | **Best Practices** | |
| **Intrusion-Detection System (IDS)** | Both network- and host-based intrusion-detection systems should be deployed to detect and notify of attacks against corporate systems. | |
|  | **Findings** | **Recommendations** |
| **Intrusion-Detection System (IDS)** | You have indicated that you are not using intrusion-detection hardware or software. | Consider deploying either host- or network-based intrusion-detection systems. |
| **Subcategory** | **Best Practices** | |
| **Wireless** | Best practice for wireless implementation should include ensuring that the network does not broadcast its SSID; that WPA encryption is used; that the network is fundamentally treated as untrustworthy. | |
|  | **Findings** | **Recommendations** |
| **Wireless** | You have indicated that wireless connectivity to the network is not available | By not currently allowing wireless access, you minimize exposure. However if wireless is planned for or implemented in the future, the implementation should include non-broadcast of SSID, WPA encryption, and treating the network as untrusted. |

|  |  |  |
| --- | --- | --- |
| **Perimeter Defense - Resources** | | |
| Windows Server 2008 | Windows Server 2008 is the most secure Windows Server yet. The operating system has been hardened to help protect against failure and several new technologies help prevent unauthorized connections to your networks, servers, data, and user accounts. Network Access Protection (NAP) helps ensure that computers that try to connect to your network comply with your organization's security policy. Technology integration and several enhancements make Active Directory services a potent unified and integrated Identity and Access (IDA) solution and Read-Only Domain Controller (RODC) and BitLocker Drive Encryption allow you to more securely deploy your AD database at branch office locations. | <http://www.microsoft.com/windowsserver2008/en/us/overview.aspx> |
| Internet Security and Acceleration Server | Internet Security and Acceleration (ISA) Server 2006 is the integrated edge security gateway that helps protect IT environments from Internet-based threats while providing users with fast and secure remote access to applications and data.Deploy ISA Server 2006 for Secure Remote Access, Branch Office Security, and Internet Access Protection. | <http://www.microsoft.com/forefront/edgesecurity/default.mspx> |
| Intelligent Application Gateway | Microsoft's Intelligent Application Gateway (IAG) 2007 is the comprehensive, secure remote access gateway that provides secure socket layer (SSL)-based application access and protection with endpoint security management. IAG 2007 enables granular access control, authorization, and deep content inspection from a broad range of devices and locations to a wide variety of line-of-business, intranet, and client/server resources. | <http://www.microsoft.com/forefront/edgesecurity/iag/default.mspx> |
| Network Access Protection | Network Access Protection (NAP) is a new platform and solution that controls access to network resources based on a client computer identity and compliance with corporate governance policy. NAP allows network administrators to define granular levels of network access based on who a client is, the groups to which the client belongs, and the degree to which that client is compliant with corporate governance policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access. | <http://technet.microsoft.com/en-us/network/bb545879.aspx> |

|  |  |  |
| --- | --- | --- |
| **Authentication** | | |
| **Subcategory** | **Best Practices** | |
| **Administrative Users** | For administrative accounts, implement a strict policy that requires the use of complex passwords that meet the following criteria:  + Alphanumeric + Upper and lower case + At least one special character + Minimum length of 14 characters  To further mitigate the risk of a password attack, implement the following controls:  + Password expiration + Account lockout after 7 to 10 failed login attempts + System logging  In addition to implementing complex passwords, consider implementing multifactor authentication. Implement advanced controls around account management (do not allow account sharing) and account-access logging. | |
|  | **Findings** | **Recommendations** |
| **Administrative Users** | You have indicated that separate logins are used for secure administration of systems and devices within the environment. | Continue requiring separate accounts for administrative/management activity, and ensure that administrative credentials are changed frequently. |
| **Administrative Users** | You have indicated that users have been granted administrative access to their workstations. | Consider removing administrative access for users, in order to limit the ability to modify the secure build. |
| **Administrative Users** | Your answers indicate that only complex password authentication is required for administrative access to manage devices and hosts. | Consider implementing an additional factor of authentication; doing so significantly reduces the risk of unauthorized access. Consider implementing advanced controls around account management and account access logging. |
| **Subcategory** | **Best Practices** | |
| **Internal Users** | For user accounts, implement a policy that requires the use of complex passwords that meet the following criteria:  + Alphanumeric + Upper and lower case + At least one special character + Minimum length of 8 characters  To further mitigate the risk of a password attack implement the following controls:   + Password expiration + Account lockout after at least 10 failed login attempts + System logging  In addition to complex passwords, consider implementing multifactor authentication.  Implement advanced controls around account management (do not allow sharing of accounts) and account-access logging. | |
|  | **Findings** | **Recommendations** |
| **Internal Users** | Your answer indicates that currently only complex password authentication is required for user access to the internal network and hosts. A password is considered complex if it meets the following criteria: + Alpha-numeric + Upper and lower case + At least one special character + Minimum length of 8 characters | Consider implementing an additional factor of authentication, which would significantly reduce the risk of unauthorized access being gained through a user account. Consider implementing advanced controls around account management and account access logging. |
| **Subcategory** | **Best Practices** | |
| **Remote-Access Users** | Implement complex password controls for all users of remote access, whether this access is granted through the use of dial-up or VPN technologies. A password is considered to be complex if it meets the following criteria:  + Alphanumeric + Upper and lower case + At least one special character + Minimum length of 8 characters  Implement an additional factor of authentication for accounts that are granted remote access. Also consider implementing advanced controls around account management (do not allow sharing of accounts) and account access logging.  In the case of remote access, it is especially important to protect the environment through the use of strong account management practices, sound logging practices, and incident detection capabilities. To further mitigate the risks of brute-force password attacks, consider implementing the following controls:   + Password expiration + Account lockout after 7 to 10 failed login attempts + System logging  Remote-access services should also take into account systems that will be used to access the network or hosts. Also consider implementing controls around hosts that are allowed to access the network via remote access. | |
|  | **Findings** | **Recommendations** |
| **Remote-Access Users** | You have indicated that employees are able to remotely connect to the network. | If you have not already done so, consider using a multifactor authentication system for remote access, and limit access to only those employees that have a business need for remote connectivity. |
| **Remote-Access Users** | You have indicated that contractors are not able to remotely connect to the network. | By not allowing remote access, you reduce your overall risk. However if remote access is planned or implemented in the future, be sure to follow best practice when deploying the remote-access solution in order to minimize the risk associated with that access. |
| **Remote-Access Users** | You have indicated that third parties are not able to remotely connect to the network. | By not allowing remote access, you reduce your overall risk. However if remote access is planned or implemented in the future, be sure to follow best practice when deploying the remote-access solution in order to minimize the risk associated with that access. |
| **Remote-Access Users** | Your answer indicated that currently only complex password authentication is required for a user that remotely accesses the internal network and hosts. A password is considered complex if it meets the following criteria: + Alphanumeric + Upper and lower case + At least one special character + Minimum length of 8 characters | Consider implementing an additional factor of authentication for accounts that are granted remote access. Also, consider implementing advanced controls around account management and account access logging. In the case of remote access it is especially important to protect the environment through the use of strong account management practices, sound logging practices, and incident detection capabilities. |
| **Subcategory** | **Best Practices** | |
| **Password Policies** | The use of complex passwords for all accounts is a basic element of Defense-in-Depth. Complex passwords should be 8 to 14 characters in length, with alphanumeric and special characters. Minimum length, history maintenance, lifetime, and pre-expiration of passwords should all be set to provide additional defenses. In general, password expiration should be set to the following:  + Maximum length 90 days + New accounts must change password at login + Password history of 8 passwords (8 days minimum)  In addition to complex passwords, multifactor authentication is important, especially for administrative and remote user accounts.  Account lockout, after 10 failed login attempts, should be enabled on all user accounts. The controls around account lockout can vary from simply being focused on blocking brute-force password attacks to requiring administrator intervention to unlock.  It is considered a best practice to enable lockout for administrative accounts, at least for network access. This would not allow the account to be locked out at the console, only from across a network. This may not be appropriate for all organizations, especially those with remote locations.  For remote-access accounts, it is best to require an administrator to unlock the account, as attacks could remain undetected for a significant amount of time if other means are not being used to track authentication failures. Consider the following guidelines when implementing controls around account lockout:   + Lockout after 7 to 10 failed login attempts for administrative and remote-access accounts + Lockout after at least 10 failed login attempts for regular user accounts + Require administrative access to re-enable for administrator and remote-access accounts and automatically re-enable regular user accounts after 5 minutes | |
| **Password Policies** | Typically the restrictions around creating passwords for administrators should be greater than those for normal accounts. On Windows systems, administrative accounts (and service accounts) should be set with passwords that are 14 characters in length and use alphanumeric and special characters. | |
| **Subcategory** | **Best Practices** | |
| **Password Policies - Administrator Account** |  | |
|  | **Findings** | **Recommendations** |
| **Password Policies - Administrator Account** | You have indicated that administrator accounts have password policies implemented. | Consider implementing additional protections around administrative accounts, such as logging and monitoring services, around all successful and failed authentications. Migrate away from clear text protocols. |
| **Subcategory** | **Best Practices** | |
| **Password Policies - User Account** |  | |
|  | **Findings** | **Recommendations** |
| **Password Policies - User Account** | You have indicated that user accounts have password policies implemented. | Consider implementing logging thresholds around failed authentications so that alerts can be sent to systems administrators. Consider testing the password policies in place. |
| **Subcategory** | **Best Practices** | |
| **Password Policies - Remote-Access Account** |  | |
|  | **Findings** | **Recommendations** |
| **Password Policies - Remote-Access Account** | You have indicated that remote access accounts have password policies implemented. | Consider implementing additional security around remote-access accounts through the use of logging and monitoring services on the remote-access device/host. Consider implementing logging thresholds around failed authentications so that alerts can be sent to systems administrators. |
| **Subcategory** | **Best Practices** | |
| **Inactive Accounts** | Continue to monitor and manage inactive accounts. | |
| **Inactive Accounts** | Institute a process to include an immediate notification procedure to all system administrators for terminated staff members to ensure their accounts are disabled immediately, especially their remote access accounts. Consider implementing a process to review the current accounts of staff that transfer to another department within the organization. | |
| **Inactive Accounts** | Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information. | |
| **Inactive Accounts** | Regularly monitor relevant vendors' sites for virus signature updates and download updates to a quarantined area for testing in a lab environment. Verify that the updates do not cause any conflicts with deployed operating systems or applications before rolling out to production.  Auto-update features for anti-virus solutions should be disabled on all systems to prevent potentially damaging files from being deployed before they are tested.  For anti-virus applications, consider deploying a central console that will facilitate reporting on which systems are out-of-date or have software features disabled.  In the case of remote users who do not regularly connect to the corporate network, consider using an auto update feature. | |
| **Inactive Accounts** | Terminated staff accounts should be disabled in a timely manner, to ensure that the terminated users or other users could use the account to gain unauthorized access. If system administrators are not aware of changes in the status of a user due to transfer, they will not change or remove system or physical accesses. This could lead to unauthorized or excessive access by transferred users. | |
|  | **Findings** | **Recommendations** |
| **Inactive Accounts** | Your response indicate that your organization has a formal process for reviewing inactive user accounts. | Continue to monitor and manage inactive accounts. |
| **Inactive Accounts** | Your answer indicates that policies for virus signature updates do exist in your environment. | Regularly monitor relevant vendor and security sites for warnings on recent attacks and new virus outbreaks. Periodically audit remote users to ensure they are updating their systems. Continue based on the listed best practices. |
| **Inactive Accounts** | Your response indicate that your organization does not have a formal process for reviewing inactive user accounts. | Institute a process to include an immediate notification procedure to all system administrators for terminated staff members to ensure their accounts are disabled immediately, especially their remote access accounts. Consider implementing a process to review the current accounts of staff that transfer to another department within the organization. |
| **Inactive Accounts** | Your answer indicates that no virus signature update policy exists for your anti-virus solution. | Work on developing a policy which calls for regular updates of virus signatures to the anti-virus solution. On a regular basis scan the relevant vendor and security sites for warnings on recent attacks and virus outbreaks, and update the virus signatures for all anti-virus solution deployments.  Require remote users to regularly update their systems. |
| **Inactive Accounts** | You have indicated that you do not know the answer to this question | Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information. |

|  |  |  |
| --- | --- | --- |
| **Authentication - Resources** | | |
| Windows Server 2008 | Windows Server 2008 is the most secure Windows Server yet. The operating system has been hardened to help protect against failure and several new technologies help prevent unauthorized connections to your networks, servers, data, and user accounts. Network Access Protection (NAP) helps ensure that computers that try to connect to your network comply with your organization's security policy. Technology integration and several enhancements make Active Directory services a potent unified and integrated Identity and Access (IDA) solution and Read-Only Domain Controller (RODC) and BitLocker Drive Encryption allow you to more securely deploy your AD database at branch office locations. | <http://www.microsoft.com/windowsserver2008/en/us/overview.aspx> |
| Windows Server Active Directory | A central component of the Windows platform, Active Directory directory service provides the means to manage the identities and relationships that make up network environments. Windows Server 2003 makes Active Directory simpler to manage, easing migration and deployment. Windows Server Active Directory is already used by companies around the world to gain unified management of identities and resources across the enterprise network. Active Directory enables organizations to centrally manage and track information about users and their privileges. In addition, Active Directory Lightweight Directory Services (ADLDS), an LDAP directory service, provides organizations with flexible support for directory-enabled applications. Integration with Microsoft Federated Identity, Strong Authentication, Information Protection and Identity Lifecycle Management solutions, makes Active Directory an ideal foundation for building a comprehensive identity and access solution. | <http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx>  <http://www.microsoft.com/windowsserver2003/technologies/idm/DirectoryServices.mspx> |
| Windows Server Group Policy | Group Policy provides an infrastructure for centralized configuation management for the operating system and applications that run oh the operating system. Group Policy is supported in both Windows Server 2003 and has advanced features in Windows Server 2008 to extend the current configuration capabilites. | <http://technet2.microsoft.com/windowsserver2008/en/library/3b4568bc-9d3c-4477-807d-2ea149ff06491033.mspx?mfr=true> |
| Windows Server 2003 - Internet Authenication Services (IAS) | Internet Authentication Service (IAS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy in Windows Server 2003. As a RADIUS server, IAS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless and virtual private network (VPN) connections. As a RADIUS proxy, IAS forwards authentication and accounting messages to other RADIUS servers. In Windows Server 2008, IAS has been replaced with Network Policy Server (NPS). | <http://technet.microsoft.com/en-us/network/bb643123.aspx> |
| Windows Server 2008 - Network Policy Server (NPS) | Network Policy Server (NPS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy in Windows Server 2008. NPS is the replacement for Internet Authentication Service (IAS) in Windows Server 2003. As a RADIUS server, NPS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless and virtual private network (VPN) connections. As a RADIUS proxy, NPS forwards authentication and accounting messages to other RADIUS servers. NPS also acts as a health evaluation server for Network Access Protection (NAP). | <http://www.microsoft.com/windows/products/windowsvista/enterprise/benefits/operatingsystem.mspx?tab=Improve%20Security%20and%20Compliance> |
| Public Key Infrastructure | Microsoft Public Key Infrastructure (PKI) for Windows Server 2003 provides an integrated public key infrastructure that enables you to secure and exchange information with strong security and easy administration across the Internet, extranets, intranets, and applications. | <http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx> |
| Certificates | Windows Certificate Services (CS) provides an integrated public key infrastructure that enables the secure exchange of information. With strong security and easy administration across the Internet, extranets, intranets, and applications, CS provides customizable services for issuing and managing the certificates used in software security systems employing public key technologies. | <http://www.microsoft.com/windowsserver2003/technologies/idm/StrongAuthentication.mspx> |
| Microsoft Identity Lifecycle Manager | Microsoft Identity Lifecycle Manager 2007 (ILM 2007) provides an integrated and comprehensive solution for managing the entire lifecycle of user identities and their associated credentials. It provides identity synchronization, certificate and password management, and user provisioning in a single solution that works across Microsoft Windows and other organizational systems. As a result, IT organizations can define and automate the processes used to manage identities from creation to retirement. | <http://www.microsoft.com/windowsserver2003/technologies/idm/ILM.mspx> |

|  |  |  |
| --- | --- | --- |
| **Management and Monitoring** | | |
| **Subcategory** | **Best Practices** | |
| **Incident Reporting & Response** | Continue to have and follow formal incident response and reporting procedures. | |
| **Incident Reporting & Response** | Institute procedures for the reporting of and response to security incidents, issues, and concerns. Designate an emergency response team that includes representatives from several disciplines including technology, human resources, and legal for responding to all security incidents and issues. Consider implementing a full incident response program that includes incident response teams, containment management, event correlation and analysis, and incident response procedures. | |
| **Incident Reporting & Response** | Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information. | |
| **Incident Reporting & Response** | Maintain a build process with all vendor patches and recommended lockdown configuration. Test this process regularly. Use host-hardening procedures to patch and properly configure services and applications on each host. Disable all nonessential services and applications.  Workstations should be hardened by installing recommended patches, removing all unnecessary services and packages, and auditing file permissions.  Incorporate host-hardening steps into standard workstation build procedures. | |
| **Incident Reporting & Response** | It is important to follow documented incident reporting and response process to ensure that all issues and incidents are reviewed and assessed in a consistent manner. It is important for all users to understand their responsibility to report any security issues or incidents and for them to have a clearly defined process for reporting these issues. | |
|  | **Findings** | **Recommendations** |
| **Incident Reporting & Response** | Your answers indicate that there is no formal image or documentation used in building workstations. | Create a secure build for each type of workstation. Update these regularly with the latest service packs, hot fixes, and other hardening techniques. |
| **Subcategory** | **Best Practices** | |
| **Secure Build** |  | |
|  | **Findings** | **Recommendations** |
| **Secure Build** | You have indicated that personal firewalls have not been installed on all of the workstations in the environment. | Implement a policy which calls for periodic review of default firewall settings, so as to allow for changes in applications or services being used. |
| **Secure Build** | You have indicated that the build processes for infrastructure devices have been documented. | Implement a documented build process for infrastructure devices, and ensure that the build is kept current as new patches are released. |
| **Secure Build** | You have indicated that client-side remote access software has been installed on workstations that connect remotely to the internal network. | Consider using a single remote-access solution for the environment, if there are multiple types of solution deployed. |
| **Secure Build** | You have indicated that the build processes for servers have been documented. | Continue using a documented build process for servers, and ensure that the build is kept current as new patches are released. |
| **Secure Build** | You have indicated that disk-encryption software is used in the environment. | Continue to use disk encryption software in your environment. |
| **Secure Build** | You have indicated that the build processes for workstations and laptops have been documented. | Continue using a documented build process for workstations and laptops, and ensure that the build is kept current as new patches are released. |
| **Secure Build** | You have indicated that remote control/management software is not used in the environment. | Continue the practice of not using remote control/management software. |
| **Secure Build** | You have indicated that a password-protected screen saver is not used in the environment. | Consider requiring all users to have a password-protected screen saver with a short time-out period. |
| **Secure Build** | You have indicated that modems are not used in the environment. | Continue disabling modem and dial-up access in order to reduce the risk of having machines able to be directly dialed into. |
| **Subcategory** | **Best Practices** | |
| **Physical Security** | Continue to implement physical security access controls. | |
| **Physical Security** | Institute physical access controls to guard against unauthorized persons gaining access to the building and to sensitive information. Consider reassessing all physical access controls to ensure they are adequate and are being complied with. Increase staff awareness of the personnel access control policy and encourage the challenging of unrecognized individuals. | |
| **Physical Security** | All computer systems should be secured to prevent easy theft. Servers and networking equipment should be secured in locked cabinets in locked rooms with controlled access. | |
| **Physical Security** | Physical access should be stringently controlled, preventing unauthorized individuals access buildings, sensitive data and systems. With such access they could alter system configurations, introduce vulnerabilities into the network, or even destroy or steal equipment. | |
|  | **Findings** | **Recommendations** |
| **Physical Security** | Your response indicated that physical security controls have not been deployed to secure your organization's assets. | Immediately plan for the use of physical controls to secure access to critical systems and network components, and consider extending physical security controls to all computer equipment in the future. |

|  |  |  |
| --- | --- | --- |
| **Management and Monitoring - Resources** | | |
| Windows Server 2008 | Windows Server 2008 is the most secure Windows Server yet. The operating system has been hardened to help protect against failure and several new technologies help prevent unauthorized connections to your networks, servers, data, and user accounts. Network Access Protection (NAP) helps ensure that computers that try to connect to your network comply with your organization's security policy. Technology integration and several enhancements make Active Directory services a potent unified and integrated Identity and Access (IDA) solution and Read-Only Domain Controller (RODC) and BitLocker Drive Encryption allow you to more securely deploy your AD database at branch office locations. | <http://www.microsoft.com/windowsserver2008/en/us/overview.aspx> |
| Windows Server Active Directory | A central component of the Windows platform, Active Directory directory service provides the means to manage the identities and relationships that make up network environments. Windows Server 2003 makes Active Directory simpler to manage, easing migration and deployment. Windows Server Active Directory is already used by companies around the world to gain unified management of identities and resources across the enterprise network. Active Directory enables organizations to centrally manage and track information about users and their privileges. In addition, Active Directory Lightweight Directory Services (ADLDS), an LDAP directory service, provides organizations with flexible support for directory-enabled applications. Integration with Microsoft Federated Identity, Strong Authentication, Information Protection and Identity Lifecycle Management solutions, makes Active Directory an ideal foundation for building a comprehensive identity and access solution. | <http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx>  <http://www.microsoft.com/windowsserver2003/technologies/idm/DirectoryServices.mspx> |
| Public Key Infrastructure | Microsoft Public Key Infrastructure (PKI) for Windows Server 2003 provides an integrated public key infrastructure that enables you to secure and exchange information with strong security and easy administration across the Internet, extranets, intranets, and applications. | <http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx> |
| Certificates | Windows Certificate Services (CS) provides an integrated public key infrastructure that enables the secure exchange of information. With strong security and easy administration across the Internet, extranets, intranets, and applications, CS provides customizable services for issuing and managing the certificates used in software security systems employing public key technologies. | <http://www.microsoft.com/windowsserver2003/technologies/idm/StrongAuthentication.mspx> |
| Forefront Client Security | Forefront Client Security helps guard against emerging threats, such as spyware and rootkits, as well as traditional threats, such as viruses, worms, and Trojan horses. By delivering simplified administration through central management and providing critical visibility into threats and vulnerabilities, Forefront Client Security helps you protect your business with confidence and efficiency. Forefront Client Security integrates with your existing infrastructure software, such as Microsoft Active Directory, and complements other Microsoft security technologies for enhanced protection and greater control. | <http://www.microsoft.com/forefront/clientsecurity/en/us/overview.aspx> |
| Windows Vista - BitLocker Drive Encryption | Bitlocker Drive Encryption is a data protection feature available in Windows Vista Enterprise and Ulitmate editions and in Windows Server 2008. Bitlocker enhances data protection by bringing together drive encription and integrity checking of early boot components. | <http://www.microsoft.com/windows/products/windowsvista/features/details/bitlocker.mspx> |
| Windows Vista - Encrypted File System (EFS) | Encrypting File System (EFS) is a data protection feature in the Business, Enterprise and Ultimate editions of Windows Vista. If is userful for user-level file and folder encryption. | <http://www.microsoft.com/windows/products/windowsvista/features/details/encryptingfilesystem.mspx> |
| Windows Vista and XPsp2 - Windows Defender | Windows Defender works with Internet Explorer 7 to help make conscious choices installing software on your PS by providing always-on protection and monitoring of key system locations watching for changes that signal the installation and presence of spyware. | <http://www.microsoft.com/windows/products/windowsvista/features/details/defender.mspx> |
| Windows Firewall | Windows Firewall is a critiacal first line of defense to protect your computer against many types of malicious software. It can help stop malware before it infects your computer. Windows Firewall comes with Windows Vista and is turned on by default to protect your system as soon as windows starts. | <http://www.microsoft.com/windows/products/windowsvista/features/details/firewall.mspx> |
| Windows Security Center | Windows Security Center alers you when your security software is out of date or when your security settings should be strengthened. It displays your firewall settings and tells you whether your PC is set up to receive automatic updates from Microsoft. | <http://www.microsoft.com/windows/products/windowsvista/features/details/securitycenter.mspx> |
| Windows Live One Care | Protect, maintain, and manage your computer with Windows Live OneCare, the always-on PC-care service from Microsoft. Working quietly in the background on your computer, OneCare protects against viruses, spyware, hackers, and other unwanted intruders. New features allow for multi-PC management to form a circle of protection, printer sharing support, and centralized backup of up to three PCs covered under the same OneCare subscription. | <http://onecare.live.com/standard/en-us/default.htm> |
| ISA Server | Internet Security and Acceleration (ISA) Server 2006 is the integrated edge security gateway that helps protect IT environments from Internet-based threats while providing users with fast and secure remote access to applications and data.Deploy ISA Server 2006 for Secure Remote Access, Branch Office Security, and Internet Access Protection. | <http://www.microsoft.com/forefront/edgesecurity/iap.mspx>  <http://www.microsoft.com/forefront/edgesecurity/sra.mspx>  <http://www.microsoft.com/forefront/edgesecurity/bos.mspx> |
| ADFS | Microsoft Active Directory Federation Services (ADFS) provides the interoperability required to simplify the broad, federated sharing of digital identities and policies across organizational boundaries. Seamless yet secure, customers, partners, suppliers, and mobile employees can all securely gain access to the information they need, when they need it. ADFS Boost cross-organizational efficiency and collaboration with secure data access across companies and Improves operational efficiency with streamlined federation systems and simplified management of IDs and passwords. It boost visibility into cross-boundary processes with transparent, auditable information rights and roles and improves security with ADFS claim mapping, SAML tokens, and Kerberos authentication. ADFS helps to reduce operations costs by taking advantage of existing investments in Active Directory and security systems and eliminates the complexity of managing federation by using Active Directory as the main identity repository. | <http://www.microsoft.com/windowsserver2003/technologies/idm/federatedidentity.mspx> |
| (IPV6) Direct Connect | IPv6 is designed to solve many of the problems of the current version of IP (known as IPv4) such as address depletion, security, autoconfiguration, and extensibility. Its use will also expand the capabilities of the Internet to enable a variety of valuable and exciting scenarios, including peer-to-peer and mobile applications. Support for Internet Protocol version 6 (IPv6), a new suite of standard protocols for the Network layer of the Internet, is built into the latest versions of Microsoft Windows, which include Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP with Service Pack 2, Windows XP with Service Pack 1, Windows XP Embedded SP1, and Windows CE .NET. | <http://technet.microsoft.com/en-us/network/bb530961.aspx> |
| IPSec | Internet Protocol security (IPsec) is a framework of open standards for protecting communications over Internet Protocol (IP) networks through the use of cryptographic security services. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft implementation of IPsec is based on standards developed by the Internet Engineering Task Force (IETF) IPsec working group. IPsec is supported by the Microsoft Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP, and Windows 2000 operating systems and is integrated with the Active Directory directory service. IPsec policies can be assigned through Group Policy, which allows IPsec settings to be configured at the domain, site, or organizational unit level. | <http://technet.microsoft.com/en-us/network/bb531150.aspx> |
| 802.1 | The IEEE 802.1X standard for wired networks provides authentication and authorization protection at the network edge where a host attaches to the network. IPsec provides peer authentication and cryptographic protection of IP traffic from end-to-end. This white paper describes the security and capabilities of 802.1X for wired networks and IPsec based on industry standards and their support in Windows Server 2003, Windows Server 2008, Windows XP and Windows Vista and provides comparison information when evaluating deployment of these security technologies. | <http://technet2.microsoft.com/windowsserver/en/library/908d13e8-c4aa-4d62-8401-86d7da0eab481033.mspx?mfr=true> |

### Applications

A thorough understanding of application security requires in-depth knowledge of the basic underlying application architecture as well as a solid understanding of the application's user base. Only then can you begin identifying the potential threat vectors.  
Given the limited scope of this self assessment, a complete analysis of application architecture and thorough understanding of the user base is not possible. This assessment is meant to help you review applications within your organization and assess them from a security and availability standpoint. It examines technologies used within the environment to help enhance Defense-in-Depth. The assessment reviews the high level procedures an organization can follow to help mitigate application risk by focusing on the following areas of application security:

* Deployment & Use — Load-Balancing, Clustering, Application & Data Recovery, Third Party Independent Software Vendor, Internally Developed, Vulnerabilities
* Application Design — Authentication, Password Policies, Authorization & Access Control, Logging, and Input Validation
* Data Storage & Communications — Encryption

|  |  |  |
| --- | --- | --- |
| **Deployment and Use** | | |
| **Subcategory** | **Best Practices** | |
| **Load-Balancing** |  | |
|  | **Findings** | **Recommendations** |
| **Load-Balancing** | You have indicated that load balancers are not deployed in the environment. | Consider deploying hardware load balancers in front of the Web servers to achieve higher availability. The load balancer shows a single (virtual) IP address to the outside world, which maps to the addresses of each Web server in the cluster. |
| **Subcategory** | **Best Practices** | |
| **Clustering** |  | |
|  | **Findings** | **Recommendations** |
| **Clustering** | Your response indicates that clustering is deployed in your environment. | Implement a formal policy which requires periodic testing of the cluster failover mechanisms. |
| **Subcategory** | **Best Practices** | |
| **Application & Data Recovery** |  | |
|  | **Findings** | **Recommendations** |
| **Application & Data Recovery** | You have indicated that your organization has line of business applications | Any Line of Business applications should be periodically evaluated for security, backed up regularly, fully documented, and have contingencies in place in case they fail. |
| **Application & Data Recovery** | Your response indicates that regular testing of application and data recovery is not performed. | Perform full backups regularly. Perform regular tests of the backup and recovery mechanism that permits restoration of the application to a normal operating state. |
| **Subcategory** | **Best Practices** | |
| **Third-party independent software vendor (ISV)** | The third-party independent software vendor (ISV) should regularly provide patches and upgrades for their application, and they should explain the purpose of patches and any impact you may expect in terms of the functionality, configuration, or security of the application being patched.  The third-party ISV should clearly identify critical patches so that they can quickly be applied.   The third-party ISV should explain all of the application's security mechanisms and provide up-to-date documentation.   The organization should be aware of any configuration requirements necessary to ensure the highest level of security. | |
|  | **Findings** | **Recommendations** |
| **Third-party independent software vendor (ISV)** | You have indicated that third party vendors have not developed one or more of the key applications in your environment. | Continue to develop key applications in house, but if the decision is made to procure from a third party in the future, ensure that the third party who has developed your key software will continue to support that software, provide updates in a timely manner, and can provide you with source code in the event that the third party can no longer support the application. |
| **Subcategory** | **Best Practices** | |
| **Internally Developed** | The in-house development team should regularly provide patches and upgrades for their application, and they should explain the purpose of patches and any impact you may expect in terms of the functionality, configuration, or security of the application being patched  The development team should clearly identify critical patches so that the organization can quickly apply them.   The development team should explain all of the application's security mechanisms and provide up-to-date documentation.   The organization should be aware of any configuration requirements necessary to ensure the highest level of security.   Consider contracting with an independent third party to review the application's architecture and deployment and identify any security issues of concern. | |
|  | **Findings** | **Recommendations** |
| **Internally Developed** | You have indicated that your organization uses custom macros for office applications. | Using custom macros requires that the security settings in Office are downgraded, exposing your office applications to malicious documents. Consider limiting the ability to develop and run custom macros to only those that have a business need. |
| **Subcategory** | **Best Practices** | |
| **Vulnerabilities** | All known security vulnerabilities should be identified and patched. Regularly monitor vendor and third-party security sites for new vulnerability information and available patches.  If there are any known security vulnerabilities that do not have available patches, determine when a patch will be available and develop an interim mitigation plan to address that vulnerability.   Consider using a third party to conduct periodic assessments to evaluate the application's security design. A third-party assessment may also turn up areas where additional security mechanisms are beneficial. | |
|  | **Findings** | **Recommendations** |
| **Vulnerabilities** | Your responses indicate that procedures exist for addressing known security vulnerabilities in applications you are currently using. | These procedures should include lab testing of the patches as well as application testing after the patch has been applied, to identify conflicts that may require the patch to be rolled back. Periodically revisit these procedures and verify that they meet current application requirements. |

|  |  |  |
| --- | --- | --- |
| **Deployment and Use - Resources** | | |
| 2007 Office Security Guide | As risks from malicious attack have increased, desktop application security mechanisms have evolved. The new security model in the 2007 Microsoft Office release provides new mechanisms, settings, and features that allow your organization to achieve an effective balance between protection and productivity while minimizing user disruption. You might think that such risks come from outside your organization, and can therefore be stopped by effective network security mechanisms such as firewalls, proxy servers, and intrusion detection systems. However, many of these business risks can come from internal users and unsecured systems that are at the heart of your organization. Unless securely configured, the desktop applications that your information workers rely on to send e-mail, write documents, create presentations, and analyze data can be critical pathways for attack by malicious software (malware), including spyware, Trojan horses, viruses, and worms. | <http://www.microsoft.com/technet/security/guidance/clientsecurity/2007office/default.mspx> |
| Microsoft Rights Management Services for Windows Server 2003 | Microsoft Windows Rights Management Services (RMS) for Windows Server 2003 is information protection technology that works with RMS-enabled applications to help safeguard digital information from unauthorized use—both online and offline, inside and outside of the firewall. RMS augments an organization's security strategy by protecting information through persistent usage policies, which remain with the information, no matter where it goes. Organizations can use RMS to help prevent sensitive information—such as financial reports, product specifications, customer data, and confidential e-mail messages—from intentionally or accidentally getting into the wrong hands. This services is built into Windows Server 2008 as Active Directory Rights Management Services (ADRMS) | <http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx> |
| Windows Server 2008 - Active Directory Rights Management Services | Windows Server 2008 - Active Directory Rights Management Services (AD RMS) is an information protection technology that works with AD RMS-enabled applications (Office 2007) to help safegaurd digital information from unauthorized use. Content owners can define who can open, modify, print, forward or take other actions with the information. | <http://technet2.microsoft.com/windowsserver2008/en/library/37c240d3-8928-4267-867b-4c005b72cca21033.mspx?mfr=true> |
| Windows Server 2008 - Clustering | Failover clustering in Windows Server 2008 can help you build redundancy into your network and eliminate single points of failure. The improvements to failover clusters (formerly known as server clusters) in Windows Server 2008 are aimed at simplifying clusters, making them more secure, and enhancing cluster stability. All of which helps reduce downtime, guard against data loss, and reduce your total cost of ownership. Because they are included in the enhanced-capability editions of Windows Server 2008, such as Windows Server 2008 Enterprise and Windows Server 2008 Datacenter, Windows Server 2008 failover clusters are much less expensive than comparable systems, which can cost thousands of dollars. Ease of deployment and affordability make Windows Server 2008 an ideal high-availability solution for organizations of all sizes. | <http://www.microsoft.com/windowsserver2008/en/us/clustering-home.aspx> |
| Microsoft Security Development Lifecycle | Trustworthy Computing is a Microsoft initiative for ensuring the production of secure code. A key element of the Trustworthy Computing initiative is the Microsoft Security Development Lifecycle (SDL). The SDL is an engineering practice that is used in conjunction with standard engineering processes to facilitate the delivery of secure code. The SDL consists of ten phases that combine best practices with formalization, measurability, and additional structure, including: security design analysis, tool-based quality checks, penetration testing, final security review, post release product security management. This methodology is also available in book form through Microsoft Press. | <http://msdn.microsoft.com/en-us/library/aa969774.aspx> |

|  |  |  |
| --- | --- | --- |
| **Application Design** | | |
| **Subcategory** | **Best Practices** | |
| **Authentication** | The application should implement an authentication mechanism whose strength is commensurate with requirements governing security of data or access to functionality. Applications that rely on passwords should provide for password complexity constraints that include character mix (alpha, numeric, and symbols), minimum length, history maintenance, enforced lifetime, pre-expiration, and dictionary checking.  The application should log failed login attempts, excluding the password. Each component that provides access to data or functionality should verify the existence of proper authentication credentials.   Administrative access to systems should be protected with the strongest forms of authentication available. Typically the restrictions around password creation for administrators should be greater than those for normal accounts.  In addition to strong passwords with good password policies, for added security multifactor authentication should be considered. | |
|  | **Findings** | **Recommendations** |
| **Authentication** | Your responses indicate that multifactor authentication is being used for key applications. | To further mitigate the risks of brute-force password attacks for external applications, consider implementing the following controls: + Password expiration + Account lockout after at least 10 failed login attempts + System logging |
| **Subcategory** | **Best Practices** | |
| **Password Policies** | The use of strong passwords is a basic element of Defense-in-Depth. Strong passwords should be 8 to 14 characters in length, with alphanumeric and special characters. Minimum length, history maintenance, lifetime, and pre-expiration of passwords should all be set to provide additional defenses to password strength. In general, password expiration should be set to the following: + Maximum length 90 days + New accounts must change password at login + Password history of 8 passwords (8 days minimum)  Administrative access to systems should be protected with the strongest forms of authentication available. Typically, the restrictions around password creation for administrators should be greater than those for normal accounts—if normal accounts require a password length of 8 characters, then administrative accounts should have 14-character passwords.  Account lockout, after 10 failed login attempts, should be enabled on all user accounts. The controls around account lockout can vary from simply being focused on blocking brute-force password attacks to as complex as requiring administrator intervention to unlock. Consider the following guidelines when implementing controls around account lockout:  + Account lockout after at least 10 failed login attempts for user accounts + Require administrative access to re-enable accounts for critical applications and automatically re-enable regular user accounts after 5 minutes for other applications + 30-minute length to cache failures for regular user accounts | |
|  | **Findings** | **Recommendations** |
| **Password Policies** | Your response indicates that strong password controls are implemented across key applications. | Consider implementing logging thresholds around failed authentications so that alerts can be sent to systems administrators. Also consider extending the use of strong passwords across all applications. |
| **Password Policies** | Your response indicates that a password-expiration control is not implemented across key applications. | Consider implementing password expiration for all types of accounts for critical applications based on the guidelines mentioned in the Best Practice column. In general, password expiration should be set to the following: + Maximum length 90 days + New accounts must change password at login + Password history of 8 passwords (8 days minimum) |
| **Password Policies** | Your response indicates that account lockout controls are not implemented across key applications. | Think about implementing account lockout (after 10 failed attempts), initially for all critical external applications. The controls around account lockout can vary from being focused on blocking brute-force password attacks to as complex as requiring administrator intervention to unlock the account. Consider the following guidelines when implementing controls around account lockout: + Lockout after 10 failed login attempts + Require administrative access to re-enable accounts + 30 minute length to cache failures for regular user accounts |
| **Subcategory** | **Best Practices** | |
| **Authorization & Access Control** | Applications should implement an authorization mechanism that provides access to sensitive data and functionality only to suitably permitted users or clients. Role-based access controls should be enforced at the database level as well as at the application interface.   This will protect the database in the event that the client application is exploited.   Authorization checks should require prior successful authentication to have occurred.   All attempts to obtain access without proper authorization should be logged.   Conduct regular testing of key applications that process sensitive data and of the interfaces available to users from the Internet. Include both "black box" and "informed" testing against the application. Determine if users can gain access to data from other accounts. | |
|  | **Findings** | **Recommendations** |
| **Authorization & Access Control** | Your response indicates that key applications restrict access to sensitive data and functionality based on privileges assigned to the account. | Consider conducting focused application testing on key applications that process sensitive data and on the interfaces available to users from the Internet. Include both 'black box' and 'informed' testing against the application and test for privilege escalation. |
| **Subcategory** | **Best Practices** | |
| **Logging** | Logging should be enabled across all applications in the environment. Log file data is important for incident and trend analysis as well as for auditing purposes.  The applications should log failed and successful authentication attempts, changes to application data including user accounts, severe application errors, and failed and successful access to resources.   When writing log data, the application should avoid writing sensitive data to log files. | |
|  | **Findings** | **Recommendations** |
| **Logging** | Your answers indicate that there are currently no logs created by applications in the environment. | Work with the application vendor (ISV or in-house development team) to implement logging for key applications. When writing log data, the application should avoid writing sensitive data. Critical events, such as those mentioned in the Best Practices section, should be logged. |
| **Subcategory** | **Best Practices** | |
| **Input Validation** | The application may accept input at multiple points from external sources, such as users, client applications, and data feeds. It should perform validation checks of the syntactic and semantic validity of the input. It should also check that input data does not violate limitations of underlying or dependent components, particularly string length and character set.  All user-supplied fields should be validated at the server side. | |
|  | **Findings** | **Recommendations** |
| **Input Validation** | Your answers indicate that there are no mechanisms deployed for input data validation in applications being used in the environment. | Work with the application vendor (ISV or internal development team) to implement mechanisms to validate incoming data to prevent malicious or malformed data from being processed by the applications. These modules should initially be implemented for external applications. The validation constraints to input data should accept data that is syntactically and semantically correct and should not rely solely on screening of input for invalid characters. |
| **Subcategory** | **Best Practices** | |
| **Software Security Development Methodologies** | Continue to use software security development methodologies. | |
| **Software Security Development Methodologies** | Institute to use of software security development methodologies to increase the security of your applications. | |
| **Software Security Development Methodologies** | When using consultants or vendors in any phase of your development cycle, ensure that they are trained on the software security development methodology your organization uses or one your organization recommends. | |
| **Software Security Development Methodologies** | Your organization's full development staff should be trained on the software security development methodology your organization has chosen. This includes Development Managers, Developers, Testers and Quality Assurance Staff. | |
| **Software Security Development Methodologies** | With the evolving security threat landscape, it is important to update your software security development methodology training and threat modeling training on an annual basis. Your development staff would be required to take updated security development training each year. | |
| **Software Security Development Methodologies** | The use of security software testing tools improves your team's ability to write secure code more effectively. Output from the use of your testing tools should be incorporated into your required annual training. | |
|  | **Findings** | **Recommendations** |
| **Software Security Development Methodologies** | Your response indicates that your organization provides software security methodology training for your development staff. | Continue to use provide software security development training to your development staff. |
| **Software Security Development Methodologies** | Your response indicates that your organization has 100% of your development staff trained on a software security methodology. | Continue to use provide software security development training to your development staff. |
| **Software Security Development Methodologies** | Your response indicates that your organization requires their development staff to attend updated software security development methodology training on an annual basis. | Continue to update your software security development training to your development staff and making annual attendance required. |
| **Software Security Development Methodologies** | Your response indicates that your organization is using a security software testing tools as a part of all their security development process. | Continue to leverage security software testing tools as an instrumental part of your security development plans. |
| **Software Security Development Methodologies** | Your response indicates that your organization does not provide software security methodology training for your development staff. | Institute a software security development methodology training program to improve your staff's ability to develop secure code. |
| **Software Security Development Methodologies** | Your response indicates that your organization makes it optional for their development staff to attend updated software security development methodology training on an annual basis. | Institute updating your software security development methodology training program on an annual basis. |
| **Software Security Development Methodologies** | Your response indicates that your organization is using a security software testing tools as a part of their security development process. | Expand your usage of security software testing tools as an instrumental part of all your security development plans. |
| **Software Security Development Methodologies** | Your response indicates that your organization does not provide software security methodology training for your development staff. | Institute a software security development methodology training program to improve your staff's ability to develop secure code. |
| **Software Security Development Methodologies** | Your response indicates that your organization does not requires their development staff to attend updated software security development methodology training on an annual basis. | Institute updating your software security development methodology training program on an annual basis. |
| **Software Security Development Methodologies** | Your response indicates that your organization is not using security software testing tools as a part of their security development process. | Institute to use of security software testing tools as an instrumental part of all your security development plans. |
| **Software Security Development Methodologies** | Your response indicates that your organization is not using a software security development methodology recommended to help develop secure code. | Institute to use of software security development methodologies to increase the security of your applications. |
| **Software Security Development Methodologies** | Your response indicates that your organization does not have your development staff trained on a software security methodology to help develop secure code. | Continue to update your software security development training to your development staff and making annual attendance required. |

|  |  |  |
| --- | --- | --- |
| **Data Storage & Communications** | | |
| **Subcategory** | **Best Practices** | |
| **Encryption** | Sensitive data should be encrypted or hashed in the database and file system. The application should differentiate between data that is sensitive to disclosure and must be encrypted, data that is sensitive only to tampering and for which a keyed hash value (HMAC) must be generated, and data that can be irreversibly transformed (hashed) without loss of functionality (such as passwords). The application should store keys used for decryption separately from the encrypted data.  Sensitive data should be encrypted prior to transmission to other components. Verify that intermediate components that handle the data in clear-text form, prior to transmission or subsequent to receipt, do not present an undue threat to the data. The application should take advantage of authentication features available within the transport security mechanism.   Examples of widely accepted strong ciphers are 3DES, AES, RSA, RC4, and Blowfish. Use 128-bit keys (1024 bits for RSA) at a minimum. | |
|  | **Findings** | **Recommendations** |
| **Encryption** | Your response indicates that key applications in your environment are encrypting sensitive data prior to transmission. Your answer indicates that key applications in your environment do encrypt sensitive data that is in storage. | Use industry-standard encryption algorithms for all encryption. |
| **Subcategory** | **Best Practices** | |
| **Encryption - Algorithm** | The application should use industry-standard cryptographic algorithms with keys of appropriate sizes and cryptographic modes appropriate to the need.  Industry recognized strong ciphers include 3DES, AES, RSA, Blowfish, and RC4.   A minimum key size of 128 bits (1024 bits for RSA) should be used. | |
|  | **Findings** | **Recommendations** |
| **Encryption - Algorithm** | You have indicated that you are using AES4/Rijndael encryption. | Continue to use your current encryption, but ensure that you are using strong keys. |
| **Encryption - Algorithm** | You have indicated that you are using the MD5 hashing algorithm. | There are weaknesses in both MD5 and SHA-1, but there is not yet a viable alternative. Once one is announced, consider migrating to the new technology. |
| **Encryption - Algorithm** | You have indicated that you are using the SHA-1 hashing algorithm. | There are weaknesses in both MD5 and SHA-1, but there is not yet a viable alternative. Once one is announced, consider migrating to the new technology. |

### Operations

This area of analysis examines the operational practices, procedures, and guidelines followed by the organization to help enhance Defense-in-Depth. This assessment examines policies and procedures that govern system builds, network documentation, and the use of technology within the environment. It also includes supporting activities required to manage the information and procedures used by the administrators and operations staff within the environment. By establishing operational practices, procedures, and guidelines that are understood and followed, an organization can potentially enhance its Defense-in-Depth posture. The assessment reviews high level procedures an organization can follow to help mitigate operations risk by focusing on the following areas of operations security:

* Environment — Firewall Rules & Filters, Administrative Users, Management Host, Disaster Recovery & Business RP, Third Party Relationships
* Security Policy — Data Classification & Disposal, Protocols & Services, Acceptable Use, User Account Management, Governance, Security Policies
* Patch & Update Management — Network Documentation, Application Data Flow, Patch & Change Management
* Backup & Recovery — Log Files, Backup, and Restore

|  |  |  |
| --- | --- | --- |
| **Environment** | | |
| **Subcategory** | **Best Practices** | |
| **Management Host** | When management packages are used, the administrative consoles should be hardened and physically secured. Harden the management workstations used to manage the network servers and devices.  Use SSH or VPN connections to protect clear-text protocols.  Management workstations should be dedicated to specific network and host administrators.  Test all management systems that utilize SNMP to ensure that they are patched to the latest version and do not use default community strings.  Shared systems do not store any management-specific data. Shared workstations are not used to administer network devices or hosts. | |
| **Subcategory** | **Best Practices** | |
| **Management Host - Servers** |  | |
|  | **Findings** | **Recommendations** |
| **Management Host - Servers** | Your answers indicate that a dedicated management computer exists for servers. | Consider using SSH or VPN for securing clear text management protocols. |
| **Subcategory** | **Best Practices** | |
| **Management Host - Network Devices** |  | |
|  | **Findings** | **Recommendations** |
| **Management Host - Network Devices** | You indicated that a dedicated management computer for administering network devices has been deployed. | Test all management systems that utilize SNMP to ensure that they are patched to the latest version and do not use default community settings. |

|  |  |  |
| --- | --- | --- |
| **Environment - Resources** | | |
| Windows Vista - User Account Controls | User Account Controls in Windows Vista improves the safety and securty of your computer by preventing dangerous software form making changes to your computer withue your explicit consent. This also helps in prohibiting users from installing rougue programs, changing system settings and performing other tasks that are the province administrators. | <http://www.microsoft.com/windows/products/windowsvista/features/details/useraccountcontrol.mspx> |
| Data Classification and Protection Whitepaper | Data Classification and protection deals with how to apply security classifications levels to the data either on a system or in transmission. | <http://www.microsoft.com/technet/security/guidance/complianceandpolicies/compliance/rcguide/4-11-00.mspx?mfr=true> |

|  |  |  |
| --- | --- | --- |
| **Security Policy** | | |
| **Subcategory** | **Best Practices** | |
| **Data Classification** | Continue to implement data classification with corresponding protection guidelines. | |
| **Data Classification** | Define a corporate data classification scheme and provide all staff with appropriate training and guidance regarding data classification. Define useable handling and protection requirements corresponding to data classification levels. | |
| **Data Classification** | Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information. | |
| **Data Classification** | It is important to have a data classification scheme with corresponding data protection guidelines. Insufficient information “classification” and segregation can allow staff, business partners, or the public access to information that is sensitive or that they do not have a “need-to-know.” This could lead to loss of brand image or corporate embarrassment owing to unauthorized disclosure of sensitive information. Scarce resources used to secure information may also be misallocated without proper information classification. Without the staff knowing what company sensitive information is and how to protect this data, there is a high likelihood that this information may be exposed to unauthorized persons. | |
|  | **Findings** | **Recommendations** |
| **Data Classification** | Your response indicate that your organization has a data classification scheme and data protection guidelines based on that scheme. | Continue to implement data classification with corresponding protection guidelines. |
| **Data Classification** | Your answer indicates that applications are not encrypting sensitive data prior to transmission. | Consider using secure communications for transmitting sensitive information for external Internet accessible applications. Based on applicability, use of SSL and IPSec over all communication channels is encouraged. |
| **Data Classification** | Your response indicate that your organization does not have a data classification scheme or data protection guidelines based on that scheme. | Define a corporate data classification scheme and provide all staff with appropriate training and guidance regarding data classification. Define useable handling and protection requirements corresponding to data classification levels. |
| **Data Classification** | You have indicated that you do not know the answer to this question | Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information. |
| **Subcategory** | **Best Practices** | |
| **Data Disposal** | Continue to implement data disposal processes. | |
| **Data Disposal** | Define and implement procedures for the management and disposal of information in both hard copy and electronic form, such as that contained on floppy disks and harddrives. | |
| **Data Disposal** | Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information. | |
| **Data Disposal** | Formal procedures should exist so that all users know the proper practices for disposing of electronic and hardcopy information. By not providing guidance and processes for securely destroying information, the confidentiality of information could be compromised. | |
|  | **Findings** | **Recommendations** |
| **Data Disposal** | Your response indicate that your organization follows documented procedures for the disposal of data. | Continue to implement data disposal processes. |
| **Data Disposal** | Your response indicate that your organization does not follow documented procedures for the disposal of data. | Define and implement procedures for the management and disposal of information in both hard copy and electronic form, such as that contained on floppy disks and harddrives. |
| **Data Disposal** | Your answer indicates that key applications in your environment are not encrypting sensitive data in storage. | Consider encrypting sensitive data fields in the database and in the file system using industry-standard algorithms |
| **Data Disposal** | You have indicated that you do not know the answer to this question | Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information. |
| **Subcategory** | **Best Practices** | |
| **Protocols & Services** | Clearly document the standards and practices regarding which protocols and services are allowed by the organization. Access-control lists should be verified to ensure that all services allowed have a business need for the level of access granted. Identify specific IP addresses/ranges wherever possible. Servers should have their services limited to only those required by the business need. Specifics for protocol version and minimum encryption strength should also be stated in these guidelines. Enforce accepted protocol usage through the use of perimeter devices (routers, gateways, firewalls, etc.), strong authentication, and encrypted communications. | |
|  | **Findings** | **Recommendations** |
| **Protocols & Services** | Your response indicates that you have documented guidelines that govern which protocols and services are allowed on the corporate network. | Audit the documentation for allowed protocols and services and check that it conforms to the configured ACLs and firewall rules on the respective devices. Publish this information on the corporate intranet, and implement policies that govern making changes to the guidelines. |
| **Subcategory** | **Best Practices** | |
| **Acceptable Use** | An Acceptable Use policy exists to govern the appropriate use of corporate networks, applications, data, and systems. The policy should also cover digital media, printed media, and other intellectual property. | |
|  | **Findings** | **Recommendations** |
| **Acceptable Use** | You have indicated that you do not know the answer to this question | Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information. |
| **Subcategory** | **Best Practices** | |
| **User Account Management** | Individual user accounts should be created for all persons needing access to IT resources. Accounts should not be shared among users. By default, accounts should be created with the minimum required privileges enabled. Network and server administrators should have privileged (administrator) as well unprivileged accounts. Password strength should be enforced and regularly audited and all account modifications should be logged. As an individual's role changes, all account privileges should be reviewed and modified as necessary. When employment is terminated, all accounts should be disabled or removed. | |
|  | **Findings** | **Recommendations** |
| **User Account Management** | Your response indicates that policies governing individual user account management are being used within the environment. | It is important to manage individual user accounts through a list of policies mentioned in the best practice section. For a Windows-based environment, consider implementing user account management through Active Directory and periodically test password strength on these accounts. A variety of shareware, freeware, and third-party tools can be used for this.  Develop auditing practices and alerts for Microsoft Operations Manager (MOM) to track account privilege changes on Windows 2000 based servers. |
| **User Account Management** | You have indicated that administrators do not have both privileged and unprivileged accounts. | Administrators should be required to use unprivileged accounts for regular work, and only use privileged accounts when needed. |
| **Subcategory** | **Best Practices** | |
| **Governance** | Third-party audits should be performed regularly to ensure compliance with all current legal and civil governance requirements (e.g., HIPAA for healthcare; Sarbanes-Oxley for SEC-regulated firms). | |
|  | **Findings** | **Recommendations** |
| **Governance** | You have indicated that your organization has policies to govern the computing environment. | Continue developing and implementing policies for governance of the computing environment, in accordance with applicable standards (ISO17799, CoBIT, HIPAA, SOX, etc.) |
| **Subcategory** | **Best Practices** | |
| **Security Policies** | Security policies should be defined with input from management, IT, and HR; empowered by the corporate executives; and frequently updated to reflect current best practice (such as CoBIT). | |
|  | **Findings** | **Recommendations** |
| **Security Policies** | You have indicated that an information security policy exists to govern the security-related activity of the organization. | Continue usage of the information security policy, but periodically review and update the policy to reflect current technologies and environment changes. |
| **Security Policies** | You have indicated that the policy was developed both by IT and business representatives. | Continue the practice of having policies developed both by IT and business representatives during future updates and revisions to the policy. |

|  |  |  |
| --- | --- | --- |
| **Patch & Update Management** | | |
| **Subcategory** | **Best Practices** | |
| **Network Documentation** | Current and accurate physical and logical diagrams of the external and internal networks should always be available.  Any changes made to the environment should be reflected in the corresponding diagrams in a timely manner.   Access to the latest diagrams should be restricted to the IT operations team. | |
|  | **Findings** | **Recommendations** |
| **Network Documentation** | Your answer indicates that logical network diagrams exist for your environment and they are kept up-to-date. | Review the policy that governs updates to the network diagrams. If change control policy exists for the environment, include updates to the diagram as a formal step in the change control policy.  Make certain the latest diagrams are only available to restricted personnel, primarily the IT operations and security team. |
| **Subcategory** | **Best Practices** | |
| **Application Data Flow** | Application architecture diagrams should depict major components and data flows that map the flow of critical data through the environment, including the systems through which the data passes and how the data is manipulated.  As changes are made to the application or the environment that hosts the application, the diagrams should be updated in a timely manner. | |
|  | **Findings** | **Recommendations** |
| **Application Data Flow** | Your response indicates that application architecture and data-flow diagrams exist for both the internal and external applications in your environment. | Review the policy that governs updates to the application diagrams. If change control policy exists for the environment, include updates to the diagram as a formal step in the change control policy. |
| **Subcategory** | **Best Practices** | |
| **Patch Management** | Security patches and configuration changes should be deployed in a timely fashion (defined by corporate security policy) from when they become available. Whether developed internally or supplied by a third-party, patches and updates should be thoroughly tested in a lab environment before being rolled into production. Additionally, each system should be tested after the patch has been applied to identify conflicts which are unique to that system and may require rollback of the patch.  Systems should be categorized to allow for scheduling based on groupings—critical systems and those exposed to higher traffic should be patched first. | |
|  | **Findings** | **Recommendations** |
| **Patch Management** | You have indicated that patches and updates are tested before being applied to all systems. | Continue testing all patches and updates before they are deployed into the production environment. |
| **Patch Management** | Your answer indicates that a patch & update policy exists both for applications and operating systems. | Continue with your current practice and review the information in the best practice section to make any required changes to your policies. Consider evaluation of SMS and WSUS for automated administration and deployment of patches for Windows servers. |
| **Subcategory** | **Best Practices** | |
| **Change Management and Configuration** | Any changes to the production environment should first be tested for security and compatibility before being released into production, and full documentation should be kept of the configuration of all production systems. | |
|  | **Findings** | **Recommendations** |
| **Change Management and Configuration** | You have indicated that your organization has a change and configuration management process. | Continue using a formal change and configuration management process to test and document all updates before deployment. |
| **Change Management and Configuration** | You have indicated that configurations are documented for reference. | Continue to document all configurations for ease of troubleshooting and restoration of systems. |
| **Change Management and Configuration** | You have indicated that changes to configurations are tested before deployment to production systems. | Continue the practice of testing all configuration changes before deployment to production systems. |
| **Change Management and Configuration** | You have indicated that configuration compliance is checked and enforced centrally. | Continue the practice of checking for and enforcing compliance through a central management system. |

|  |  |  |
| --- | --- | --- |
| **Patch & Update Management - Resources** | | |
| Microsoft Update | Microsoft provides an automatic way for you to get the latest product updates and security patchs on regular basis through our Microsoft Update service. | <http://www.update.microsoft.com/microsoftupdate/v6/vistadefault.aspx?ln=en-us> |
| Microsoft Windows Server Update Services | Microsoft Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates to computers running the Windows operating system. By using WSUS, administrators can fully manage the distribution of updates that are released through Microsoft Update to computers in their network. | <http://technet.microsoft.com/en-us/wsus/default.aspx> |
| Systems Center Configuration Manager | System Center Configuration Manager 2007 is the solution to comprehensively assess, deploy, and update your servers, clients, and devices across physical, virtual, distributed, and mobile environments. Optimized for Windows and extensible beyond, it is the best choice for gaining enhanced insight into and control over your IT systems. | <http://www.microsoft.com/systemcenter/configurationmanager/en/us/default.aspx> |

|  |  |  |
| --- | --- | --- |
| **Backup and Recovery** | | |
| **Subcategory** | **Best Practices** | |
| **Log Files** | Log files are configured to allow for recording all planned activity without overwriting entries. An automated process should be set up to rotate log files on a daily basis and offload the logs to a secure server within the management network. Access to log files and configuration settings should be restricted to prevent modification and deletion.  Log files should be reviewed regularly to ensure that suspicious or anomalous activity is identified. Review should include systems operation, maintenance, and security. Event correlation software and trend analysis should be used to enhance review capability. | |
|  | **Findings** | **Recommendations** |
| **Log Files** | You have indicated that log files are rotated in your environment. | Consider storing the log files in a database so that the security team can perform trend analysis and have access to protected logs in the event an incident occurs. |
| **Log Files** | You have indicated that log files are reviewed regularly in your environment. | Consider having the log files from the DMZ and core network servers monitored by MOM (Microsoft Operations Manager). In the event of critical log-file entries being generated, MOM will send alerts to the appropriate members of the team. |
| **Log Files** | You have indicated that access to log files is protected in your environment. | Consider offloading log files to a secure server within the management network for archiving purposes. Access to the archived log files should be restricted to the security team for incident analysis. |
| **Log Files** | You have indicated that logs are written to a centralized log server. | Continue logging to a centralized log server. |
| **Subcategory** | **Best Practices** | |
| **Disaster Recovery & Business Resumption Planning** | Continue to maintain and test disaster recovery / business resumption plans. | |
| **Disaster Recovery & Business Resumption Planning** | Require disaster recovery plans to be developed, documented, implemented, and subjected to periodic reviews, tests, and updates. Develop Business Continuity Plans that include staff, locations, as well as systems and other technology issues. | |
| **Disaster Recovery & Business Resumption Planning** | Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information. | |
| **Disaster Recovery & Business Resumption Planning** | Disaster Recovery and Business Resumption plans should be well documented and up-to-date, to ensure recovery in an acceptable timeframe. Plans (including restore from backup for applications) should be regularly tested to validate correctness and completeness. Business Continuity Plans should focus on the entire environment; physical, technological, and staff. | |
|  | **Findings** | **Recommendations** |
| **Disaster Recovery & Business Resumption Planning** | Your response indicate that your organization maintains procedures for Disaster Recovery and Business Resumption. | Continue to maintain and test disaster recovery / business resumption plans. |
| **Disaster Recovery & Business Resumption Planning** | Your response indicate that your organization does not maintain procedures for Disaster Recovery and Business Resumption. | Require disaster recovery plans to be developed, documented, implemented, and subjected to periodic reviews, tests, and updates. Develop Business Continuity Plans that include staff, locations, as well as systems and other technology issues. |
| **Disaster Recovery & Business Resumption Planning** | You have indicated that you do not know the answer to this question | Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information. |
| **Disaster Recovery & Business Resumption Planning** | You have indicated that you do not know the answer to this question | Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information. |
| **Subcategory** | **Best Practices** | |
| **Backup** | Full backups should be performed at regular intervals. If feasible, partial intermediary backups should be made between full backups. The backup strategy should address the worst-case scenario of a complete system and application restore. For critical applications, the restore process should result in a fully functioning application in minimal time. | |
|  | **Findings** | **Recommendations** |
| **Backup** | Your answer indicates that critical assets in your environment are being backed up on a regular basis. | Audit the backup mechanisms and ensure that all critical assets are being backed up regularly. Periodically test the restore functionality to verify recoverability from the backup media. |
| **Subcategory** | **Best Practices** | |
| **Backup Media** | Detailed policies should exist to govern the storage and handling of backup media. These policies should address issues such as: + Onsite/Offsite Storage  + Media Rotation  + Security Controls  + Personnel Access Controls   Removable backup media should be stored in locked, fire-proof cabinets and only authorized personnel should have access to these cabinets.   Offsite storage locations should be used to offer greater recoverability in the event of disaster. | |
|  | **Findings** | **Recommendations** |
| **Backup Media** | Your response indicates that a policy which addresses the storage and handling of backup media does exist in your environment. | While just having a policy in place to govern the handling and storage of backup media is a great first step, it is important to have this policy be thorough and well defined. Regularly audit the policy to ensure that it meets all of the criteria outlined in the best practice section. |
| **Backup Media** | You have indicated that backups are not stored in locked fireproof cabinets. | Backup media should be kept in a locked, fireproof cabinet offsite, have its access restricted only to necessary personnel, and rotated and replaced in accordance with manufacturer's recommendations. |
| **Subcategory** | **Best Practices** | |
| **Backup & Restore** | Backup and restore procedures should be tested regularly to identify faulty media and improve the chance of a successful restore in the event of an outage. Detailed procedures for restoring different systems, including applications, should be well-documented.   Audit all the backup and restore documents to ensure all the critical systems necessary for business continuity are covered. | |
|  | **Findings** | **Recommendations** |
| **Backup & Restore** | Your answer indicated that a well-documented policy exists for backup & restore procedures. | Audit all the backup and restore documents to ensure all the critical systems necessary for business continuity are covered. Test backup and recovery process on a regular basis to ensure that all hardware and software components are functioning as expected. |

### People

Security efforts in an organization often overlook organizational aspects that are critical to helping the organization maintain overall security. This section of the assessment reviews those processes within the enterprise governing corporate security policies, Human Resources processes, and employee security awareness and training. The People Area of Analysis also focuses on dealing with security as it relates to day-to-day operational assignments and role definitions. The assessment reviews high- level procedures an organization can follow to help mitigate people risk by focusing on the following areas of people security:

* Requirements and Assessments — Security Requirements & Assessments
* Policy and Procedures — Background Checks, HR Policy, Third-Party Relationships
* Training and Awareness — Security Awareness & Training

|  |  |  |
| --- | --- | --- |
| **Requirements & Assessments** | | |
| **Subcategory** | **Best Practices** | |
| **Security Requirements** | The organization identifies individuals with subject-matter expertise in security to be involved in all security-related discussions and decisions. The organization identifies what it needs to protect based on the value of the asset, as well as the level of security needed to protect it. All threat vectors are included in the analysis. The resulting strategy balances cost and benefit of the protections, and may include transfer or acceptance of risk as an option. Security requirements, derived from both business and technical representatives, are documented and published for all parties to review and address in future designs. Differences between classes of applications and data may result in different end requirements being identified. | |
|  | **Findings** | **Recommendations** |
| **Security Requirements** | You have indicated that your organization has a model for assigning criticality levels to each component of the computing environment. | Continue to assign levels of criticality to components, and be sure to update the model as new equipment is added. |
| **Subcategory** | **Best Practices** | |
| **Security Assessments** | Third-party assessments should be conducted to gain a valuable and objective view of an organization's security posture. Third-party assessments might also prove beneficial in meeting regulatory, customer, partner, and vendor requirements.   Assessments should cover infrastructure, applications, policies, and audit procedures. These assessments should focus not solely on identifying vulnerabilities, but also on auditing for non-secure configurations and extraneous access privileges. Security policies and procedures should be reviewed and evaluated for gaps. | |
|  | **Findings** | **Recommendations** |
| **Security Assessments** | Your answer indicates that independent security assessments are currently being performed at your organization. | Independent assessments provide significant value to an organization. Be sure to continue having third-party assessments conducted at regular intervals. If there is a substantial change in the design and configuration of your environment, consider scheduling a security assessment as soon as possible. |
| **Security Assessments** | You have indicated that you do not know the answer to this question | Review this open item with your IT staff or a security partner. Input the most appropriate answer to this question in the MSAT for further information. |

|  |  |  |
| --- | --- | --- |
| **Policy & Procedures** | | |
| **Subcategory** | **Best Practices** | |
| **Background Checks** | Background checks should be performed to identify any potential issues, thus reducing the risk exposure to the organization and to other employees. This step also helps identify any potential issues and gaps in the candidate's resume.  The hiring process should include a review of the candidate's employment and legal history.   A candidate's skills should be evaluated against detailed job descriptions and task requirements to understand strengths and weaknesses. | |
|  | **Findings** | **Recommendations** |
| **Background Checks** | Your answer indicates that background checks are being performed for all employees. | Excellent, continue this policy. Ensure that the background check includes a review of the candidate's employment, education, and legal history. |
| **Subcategory** | **Best Practices** | |
| **Human Resources Policy** | Formal exit procedures ensure that all the necessary steps are undertaken when an employment contract is terminated.  These procedures should exist to handle both friendly and unfriendly employee exits.   These procedures should include:  + Notification to all departments—Human Resources, IT, Physical Security, Help Desk, Finance, etc.  + Escorting the employee from the premises  + Termination of all accounts and network access  + Collection of company property—laptop, PDA, electronic media, confidential documents, etc. | |
|  | **Findings** | **Recommendations** |
| **Human Resources Policy** | Your response indicates that a formal hostile-employee exit policy exists within your organization. | Regularly review existing hostile employee exit procedures and update for gaps based on past terminations. |
| **Human Resources Policy** | Your response indicates that a friendly employee exit policy exists within your organization. | Periodically review the existing friendly employee exit procedure and evaluate any gaps that are discovered. |
| **Subcategory** | **Best Practices** | |
| **Third-Party Relationships** | To help reduce the risk of exposure, formal policies and procedures should exist to govern relationships with third parties. These policies and procedures help to identify security issues and the responsibilities of each party in mitigating them.  These policies should include:  + Level of connectivity and access  + Data presentation and manipulation  + Roles and responsibilities (including authority) of each party  + Management of the relationship—setup, ongoing, and termination. | |
|  | **Findings** | **Recommendations** |
| **Third-Party Relationships** | You have indicated that your organization manages the computing environment itself. | Based on business needs, either self management or outsourcing can be viable solutions. If the management is outsourced, security requirements should be addressed in the contract, and service-level agreements (SLAs) used to enforce compliance with those requirements. |
| **Third-Party Relationships** | Your answer indicates that policies do exist which govern third-party relationships. | Audit all the polices and procedures for existing third-party relationships. Revisit these policies as the business evolves to ensure they are still aligned and properly represent the position of your company. |
| **Third-Party Relationships** | You have indicated that systems are configured by the hardware supplier or a reseller. | In order to minimize the risk of having default services running, systems should be configured by internal staff following a tested build image. |

|  |  |  |
| --- | --- | --- |
| **Training & Awareness** | | |
| **Subcategory** | **Best Practices** | |
| **Security Awareness** | A security awareness program helps employees contribute to a company's overall security posture by keeping them up-to-date on security risks. Knowledgeable employees are your best source for reporting security issues. An effective awareness program should take into account all aspects of security—including application, network, and physical—while providing clear guidelines for what employees should do if they witness things that appear to jeopardize the security of any of these elements.   Implement policies that regulate employee usage of company resources.   Awareness programs should be a part of new employee orientation. Updates and refresher courses should be conducted regularly to ensure all employees are aware of the most current practices and risks.    Periodic testing should be implemented to ensure employees have absorbed the material. | |
|  | **Findings** | **Recommendations** |
| **Security Awareness** | Your response indicates that a security awareness program does exist at your organization. | All employees should participate in security awareness training. Security awareness should be mandatory as part of new employee orientation. Knowledgeable employees are your best source for reporting security issues. |
| **Security Awareness** | You have indicated that you do not have an individual or group responsibility for security at your organization. | Designate a person or group with expertise in security to be responsible for security for the company, and require that this individual/team is consulted before changes are made to the computing environment. |
| **Security Awareness** | You have indicated that awareness training does not cover privacy issues. | Security awareness training should cover all aspects of security, including security policies and controls, reporting suspicious activity, privacy, e-mail security, Internet security, and computer security. |
| **Security Awareness** | You have indicated that training is provided annually. | Security training should be provided for all employees on a quarterly basis. |
| **Security Awareness** | You have indicated that greater than 75% of all employees have participated in a security awareness program. | Continue requiring that all employees should participate in security awareness training. Security awareness should be mandatory as part of new employee orientation. Knowledgeable employees are your best source for reporting security issues. |
| **Subcategory** | **Best Practices** | |
| **Security Training** | Work with business owners to determine the acceptable downtime for critical applications. Based on those findings take appropriate measures to meet or even surpass those requirements. Availability and performance of Web-based applications is improved by deploying load balancers in front of the Web servers. To balance server load, a load balancer distributes requests to different nodes within a server cluster with the goal of optimizing system performance. If one Web server in a server cluster fails, then the request is directed to another server to handle the request, providing high availability.  Determine acceptable downtime for critical file shares and databases from business owners. Test the failover mechanisms for the applications, and determine if the amount of downtime is acceptable. To minimize downtime, a clustering mechanism should be deployed. Each instance of the clustered application participates in the same security domain, i.e., shares a common user and group database. Management operations within the cluster of machines and within the application instances take effect both in the individual instance and across its peers. Applications that rely on special knowledge of the clustering environment--such as through interactions with load balancers--recognize and handle all foreseeable exception conditions. Appropriate responses include alerting operations staff and effecting a smooth failover.    The backup strategy should address worst-case scenarios of a complete system and application restore. For critical applications, the restore process should result in a fully functioning application in minimal time. Perform regular tests of the backup/recovery mechanism that permits restoration of the application to a normal operating state. | |
|  | **Findings** | **Recommendations** |
| **Security Training** | Your response indicates that subject matter related training is currently being offered to employees based on their roles in the organization. | Role-based training and continuing education are integral to ensuring all employees understand what is expected of them and how to meet those expectations. Continue to offer training to employees at all levels in the organization and across all aspects of security as their roles require. |
| **Security Training** | You have indicated that incident readiness and response training is not offered to employees based on their role in the organization. | Role based, subject matter related training should be offered to all employees in the organization. This training should be more thorough than that given to general employees, and refreshed frequently. |
| **Security Training** | You have indicated that infrastructure security training is not offered to employees based on their role in the organization. | Role based, subject matter related training should be offered to all employees in the organization. This training should be more thorough than that given to general employees, and refreshed frequently. |

|  |  |  |
| --- | --- | --- |
| **Training & Awareness - Resources** | | |
| Microsoft Security Certifications | The MCSE: Security for Windows Server2003 certification provides you the skill set to secure a Windows Server environment. | <http://www.microsoft.com/learning/mcp/mcse/security/windowsserver2003.mspx> |
| Industry Security Certifications | (ISC)2 - CISSP, SSCP Certifications ISACA - CISM, CISA Certifications CompTIA - Security+ | <http://www.isc2.org>  <http://www.isaca.org>  <http://www.comptia.org> |
| Microsoft Security Awareness Toolkit | Microsoft recognizes that information security awareness and training is critical to any organization's information security strategy and supporting security operations. People are in many cases the last line of defense against threats such as malicious code, disgruntled employees, and malicious third parties. Therefore, people need to be educated on what your organization considers appropriate security-conscious behavior, and also what security best practices they need to incorporate in their daily business activities. This kit was created to provide guidance, samples, and templates for creating your own security awareness program. | <http://technet.microsoft.com/en-us/security/cc165442.aspx> |

## Prioritized Action List

The following list prioritizes the recommendations made above in the [Assessment Detail](#AssessmentInDetial)section. For more information on any of these items, refer to the matching entry in that section.

A Microsoft security partner can help with building a security program that encompasses these actions.[Assessment Detail](#AssessmentInDetial)section. For more information on any of these items, refer to the matching entry in that section.

|  |  |  |
| --- | --- | --- |
| **Prioritized Action List** | | |
| ***Analysis Topic*** | | ***Recommendation*** |
| **High Priority** | | |
| People > Policy & Procedures > Third-Party Relationships | In order to minimize the risk of having default services running, systems should be configured by internal staff following a tested build image. | |
| Applications > Deployment and Use > Vulnerabilities | These procedures should include lab testing of the patches as well as application testing after the patch has been applied, to identify conflicts that may require the patch to be rolled back. Periodically revisit these procedures and verify that they meet current application requirements. | |
| People > Requirements & Assessments > Security Assessments | Independent assessments provide significant value to an organization. Be sure to continue having third-party assessments conducted at regular intervals. If there is a substantial change in the design and configuration of your environment, consider scheduling a security assessment as soon as possible. | |
| People > Requirements & Assessments > Security Requirements | Continue to assign levels of criticality to components, and be sure to update the model as new equipment is added. | |
| Applications > Deployment and Use > Application & Data Recovery | Any Line of Business applications should be periodically evaluated for security, backed up regularly, fully documented, and have contingencies in place in case they fail. | |
| **Medium Priority** | | |
| People > Training & Awareness > Security Awareness | Designate a person or group with expertise in security to be responsible for security for the company, and require that this individual/team is consulted before changes are made to the computing environment. | |
| Applications > Data Storage & Communications > Encryption | Use industry-standard encryption algorithms for all encryption. | |
| Applications > Data Storage & Communications > Encryption - Algorithm | Continue to use your current encryption, but ensure that you are using strong keys. | |
| Infrastructure > Authentication > Administrative Users | Consider implementing an additional factor of authentication; doing so significantly reduces the risk of unauthorized access. Consider implementing advanced controls around account management and account access logging. | |
| Applications > Application Design > Software Security Development Methodologies | Continue to use provide software security development training to your development staff. | |
| **Low Priority** | | |
| Operations > Environment > Management Host - Servers | Consider using SSH or VPN for securing clear text management protocols. | |
| Operations > Environment > Management Host - Network Devices | Test all management systems that utilize SNMP to ensure that they are patched to the latest version and do not use default community settings. | |
| Operations > Backup and Recovery > Backup | Audit the backup mechanisms and ensure that all critical assets are being backed up regularly. Periodically test the restore functionality to verify recoverability from the backup media. | |
| Infrastructure > Perimeter Defense > Anti-virus - Desktops | Continue the practice. Implement a policy that requires users to regularly update virus signatures. Consider adding the anti-virus client in the default workstation build environment. | |
| Infrastructure > Perimeter Defense > Anti-virus - Servers | Continue the practice. Consider actively managing anti-virus clients on the servers from a centralized management console for configuration and signature deployment. If you are using Microsoft Exchange, consider using the additional anti-virus and content filtering capabilities at the mailbox level. | |

## Appendices

### Questions and Answers

The following answers were provided for input into this assessment.

|  |  |
| --- | --- |
| **Assessment Question** | **Your Answer** |
| **Business Risk Profile** | |
| Number of desktops and laptops in use at your company: | Fewer than 50 |
| Number of servers in use at your company: | 1 to 5 |
| Does your company maintain a full-time connection to the Internet? | Yes |
| Do customers and vendors access your network or internal systems via the Internet? | Yes |
| Does your company host application services, such as a portal or a Web site, for external customers or partners? | Yes |
| Does your organization deploy services that are used by both external and internal clients in the same network segment? | Yes |
| Do external partners or customers connect directly to your company's internal, back-end systems for the purposes of data access, record updates, or other information manipulation? | No |
| Has your organization deployed the same back-end infrastructure components, such as databases, to support both external applications and internal corporate services? | No |
| Does your organization allow employees or contractors to connect remotely to the internal corporate network? | Yes |
| Does your organization allow employees to deploy non-production systems, such as personal Web servers or computers housing "pet projects," on the general corporate network? | No |
| Aside from backup tapes/media, does your organization allow confidential or proprietary data off-site for processing? | Yes |
| Would a compromised system's security significantly impact your company's ability to conduct business? | Yes |
| Does your company share office space with other organizations? | No |
| Does your company develop applications? | Yes |
| Does your organization allow software developers to connect remotely to corporate development resources or remotely develop application code? | Yes |
| Does your company develop and market software products for customers, partners, or a broad market? | Yes |
| Does your organization allow developers to run development or test systems in remote or unprotected locations? | Yes |
| Does your IT staff act as the custodian (as opposed to developer) of line of business applications? | Yes |
| Do your business processes require data that is stored, processed, or distributed by a third party? | Yes |
| Does your company store or process customer data in an environment that is shared with corporate resources? | No |
| Do you rely on third-party software development partners to support business-service offerings? | Yes |
| Does your company generate revenue based on service offerings that require data processing or data mining? | No |
| Does your organization consider the data processed by your company's application services sensitive or critical to your customers' business operations? | Yes |
| Does your company make its critical business applications available through Internet-based connections? | Yes |
| Who are the target users of the key applications within your environment? | Both internal employees and external customers, vendors, and partners |
| How is access to key applications made available to users? | Both from within the internal network and remotely |
| Does your corporate network connect to customer, partner, or third-party networks via network links, whether public or private? | Yes |
| Does your company generate revenue from services based on the storage or electronic distribution of data, such as media files or documentation? | No |
| Has your organization gone through a "rip and replace" change of any major technology component in the last 6 months? | No |
| Does your company rely on receiving data feeds or processed data from partners, vendors, or other third parties? | Yes |
| Would an incident that affected customer applications or infrastructure, such as a site outage or a hardware or application failure, impact revenue? | Yes |
| Does your company store sensitive or critical customer data? | No |
| Do customer infrastructure components or applications rely on access to resources within your environment? | Yes |
| Does your company share infrastructure and application components among multiple customers? | Yes |
| Do you consider information technology to be a requirement for your company? | Yes |
| Do all of the employees in your company use computers for business? | Yes |
| Does your company outsource maintenance or ownership of any portion of its infrastructure? | Yes |
| Does your company have a mid- or long-term plan for the selection and deployment of new technology components? | Yes |
| Do you consider your organization to be an early adopter of new technology? | Yes |
| Does your organization select and deploy new technologies based on existing partnerships and licensing agreements? | Yes |
| Does your organization limit technology choices to technologies known by the current IT staff? | Yes |
| Does your company expand its network through acquisition of new companies and their existing environments? | Yes |
| Does your organization allow employees to download sensitive customer or corporate data to their workstations? | Yes |
| Does your organization restrict access to information by users based on their role? | Yes |
| Does your organization deploy new services or applications before assessing them for possible security issues? | No |
| Does your organization change credentials for privileged accounts on a regular basis? | Yes |
| Does your organization change credentials for privileged accounts after termination of personnel with privileged access? | Yes |
| Choose the option that best describes your company's industry segment: | IT Services |
| Choose the size of your organization: | 10 to 49 employees |
| Does your company have more than one location? | No |
| Is your company in a highly competitive or research-focused industry in which intellectual property theft or espionage is a significant concern? | Yes |
| Are the technologists in your company subject to high turnover or attrition? | Yes |
| Does your company have significant product or brand recognition? | Yes |
| Does your company use down version or legacy software (software that is no longer supported by the vendor)? | No |
| Does your organization acquire software from a reputable vendor or source? | Yes |
| **Infrastructure** | |
| Does your organization use firewalls or other network-level access controls at network borders to protect corporate resources? | Yes |
| Does your organization deploy these controls at each office location? | Yes |
| Does your organization use a neutral zone (commonly referred to as a demilitarized zone or DMZ) that separates internal and external networks to host services? | No |
| Does your organization host Internet-facing services on the company's network? | No |
| Does the organization use host-based firewall software to help protect servers? | Yes |
| Does your organization use intrusion-detection hardware or software to help identify attacks? | No |
| Are anti-virus solutions implemented in the environment? | Yes |
| Please select the systems that have anti-virus solutions deployed: | E-mail servers  Perimeter hosts (gateways, proxies, relays, etc.)  Desktops  Servers |
| Is remote access to the company's network available? | Yes |
| Select who is able to connect remotely to the network: | Employees |
| Is virtual private network (VPN) technology being used to provide secure connectivity to corporate resources for these remote users? | Yes |
| Is the VPN capable of limiting connectivity to a quarantine network until the client has passed all necessary security checks? | Yes |
| Is multi-factor authentication (tokens, smart cards, etc.) required for remote users? | Yes |
| Does the network have more than one segment? | No |
| Is wireless connectivity to the network available? | No |
| Do controls exist to enforce password policies on various types of accounts? | Yes |
| Select the accounts for which controls exist to enforce password policies: | Administrator  User  Remote Access |
| Indicate the authentication option used for administrative access to manage devices and hosts: | Complex password |
| Indicate the authentication option used for internal network and host access by internal users: | Complex password |
| Indicate the authentication option used for remote access by users: | Complex password |
| Is account lockout enabled to block access to accounts after a set number of failed login attempts? | Yes |
| Does your organization have processes for reviewing inactive administrative, internal use, vendor and remote user accounts? | Yes |
| Does your company configure its systems itself or is this done by the hardware supplier/reseller? | Configured by hardware supplier/reseller |
| Which of the following are built based on either an image or a formal documented configuration? | Workstations and laptops  Servers  None |
| Does this configuration include 'host hardening' procedures? | Yes |
| Which of the following solutions have been installed on employee workstations and laptops? | Personal firewall software  Spyware detection and removal software  Disk encryption software |
| Does your organization have formal incident response procedures? | No |
| Have physical security controls been deployed to secure the company's assets? | No |
| **Applications** | |
| Does your company have line of business (LOB) applications? | Yes |
| Do you use custom macros for Office applications (such as Word, Excel, or Access)? | Yes |
| What mechanisms are in place to ensure high availability of applications? Select all the mechanisms that are deployed from the list below: | Clustering |
| Has an in-house team developed any of the key applications deployed in your environment? | No |
| Have third-party consultants/vendors developed any of the key applications deployed in your environment? | No |
| What software security development methodologies are practiced at your company? (Select all that apply) | Other |
| Does your organization know of security vulnerabilities that currently exist in any of the applications being used in the environment? | Yes |
| Does your organization have procedures in place to address these security vulnerabilities? | Yes |
| Does your company provide security training for your development and testing staff? | Yes |
| What percentage of your company's development and testing staff is trained on security development practices? | 100% |
| Does your company update the security development training provided to your development staff on an annual basis? | Yes, Required |
| Does your company rely on software tools as part of the test and audit process for secure software development? | Yes, for all projects |
| Do controls exist to enforce password policies in key applications? | Yes |
| Select the password controls that are enforced across key applications: | Complex Passwords |
| Select the most common authentication method used for key applications from the list below: | Multifactor authentication |
| Do key applications in your environment have mechanisms enabled to restrict access to sensitive data and functionality? | Yes |
| Do key applications in your environment record messages in log files for analysis and auditing purposes? | No |
| Is input data validated by the deployed applications? | No |
| Do key applications encrypt sensitive and business critical data that they process? | Yes |
| Select the different stages where encryption is used: | Transmission and Storage |
| Which of the following encryption algorithms are used? | Advanced Encryption Standard (AES4)/Rijndael  MD5 Hash  SHA-1 Hash |
| **Operations** | |
| Does the company manage the environment itself, or outsource? | The company manages the environment |
| Does the organization use dedicated management hosts for secure administration of systems and devices within the environment? | Yes |
| Select the systems for which dedicated management hosts exist: | Network devices  Servers |
| Are separate login accounts used for normal activity vs. administrative/management activity? | Yes |
| Does the organization grant users administrative access to their workstations and/or laptops? | Yes |
| Is the firewall tested regularly to ensure it performs as expected? | Yes |
| Does your organization maintain Disaster Recovery and Business Resumption Plans? | Yes |
| Are these plans regularly tested? | Yes |
| Does a model exist for assigning criticality levels to each component of the computing environment? | Yes |
| Do policies exist to govern the computing environment? | Yes |
| Does an information security policy exist to govern the security-related activity of the organization? | Yes |
| Please select who developed the policy: | IT and business representatives together |
| Does a corporate acceptable use policy exist? | I don't know |
| Do policies exist for individual user account management? | Yes |
| Select which of the following policies are being applied towards individual user account management: | Individual user accounts (accounts are not shared)  Enforce password strength  On employee exit, accounts are disabled |
| Does a documented process exist for host builds? If yes, which types? (For what host types does a documented build process exist?) | Servers  Workstations and laptops |
| Do documented guidelines exist that govern which protocols and services are allowed on the corporate network? Select the option that applies. | Guidelines exist and they are documented |
| Does your organization have a formal, well-documented process for the disposal of data on electronic media and hardcopy form? | Yes |
| Does your organization have a data classification scheme with associated data protection guidelines? | Yes |
| Does a change and configuration management process exist? | Yes |
| Does the organization have configurations documented for reference? | Yes |
| Does the organization test changes to configurations before deploying to production systems? | Yes |
| Is configuration compliance checked and enforced centrally (e.g., through Active Directory Group Policy)? | Yes |
| Does an established patch and update policy and process exist? | Yes |
| Select the components for which these exist: | Both operating systems and applications |
| Does the organization test patches and updates before deploying them? | Yes |
| Indicate which of the following are used to deploy and manage patches: | Other patch management solution(s) |
| On which host types is automated patch management used? | Workstations and laptops  Servers |
| Does an established policy exist to govern the updating of signature-based detection products? | Anti-virus  Intrusion-detection system (IDS) |
| Do accurate logical diagrams and supporting configuration documentation exist for the network infrastructure and hosts? | Yes |
| Do accurate application architecture and data flow diagrams exist for key applications? | Yes |
| For which types of applications do diagrams exist: | Both internal and external applications |
| Is logging enabled in the environment to record events on hosts and devices? | Yes |
| Does the organization take measures to protect the information contained within logs? | Operating system and applications are configured to not overwrite events  Log files are rotated frequently to ensure sufficient space is available  Access to log files is restricted to administrator-level accounts  Logs are written to a centralized log server |
| Does the organization review log files regularly? | I don't know |
| Is critical and sensitive data backed up on a regular basis? | Yes |
| Do policies and procedures exist for storage and handling of backup media? | Yes |
| Which of the following policies and procedures are followed: | Offsite storage  Restricted personnel access to backup media  Rotation and lifecycle of backup media |
| Do policies exist for regular testing of backup and restore procedures? Are these policies documented? | Yes, and they are documented |
| **People** | |
| Do you have an individual or group in your company that is responsible for security? | No |
| Does your organization perform security assessments of the environment through independent third-parties? | Yes |
| How often are these assessments performed? | Semi-annually |
| Select the areas of analysis that are being covered by these assessments: | Infrastructure  Application  Policy  Audit |
| Does your organization perform security assessments of the environment internally? | I don't know |
| Does the organization perform background checks as a component of the hiring process? | Yes |
| Please select the option that is most appropriate: | Background checks are performed for all positions |
| Does a formal employee exit process exist? | Yes |
| Select the options for which a formal employee exit policy exists: | Hostile exits  Friendly exits |
| Does a formal policy exist to govern third-party relationships? | Yes |
| Does a security awareness program exist at your company? | Yes |
| What percentage of employees have participated in the security awareness program? | Greater than 75% |
| Which of the following topics does the awareness training cover? | Company security policies and controls  Reporting suspicious activity  E-mail security, including spam and attachment handling  Internet security, including web surfing and downloads  Computer security, including use of personal firewalls and encryption |
| How frequently is training offered? | Annually |
| Is subject-matter-related training offered to employees based on their roles in the organization? | Yes |
| Select all the subjects that apply from the list below: | Operations Security  Application Security |

### Glossary

The glossary addresses standard security industry terms and concepts included in this report. Additional terms outside of this report may also be included.

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **AoAs** | Areas of Analysis which are infrastructure, applications, operations, and people. |
| **Applications** | A software program that provides functionality to an end user. Requires an operating system to run. Examples include word processor, spreadsheet, and database programs. |
| **Anti-virus (AV)** | Software and hardware technologies that protect the computing environment from malicious software. |
| **Business Risk Profile (BRP)** | A measurement of the risk to which an organization is exposed, based on the business environment and industry in which it competes. |
| **Defense-in-Depth Index (DiDI)** | A measurement of the security defenses used across people, process, and technology to help mitigate the risks identified for a business. |
| **Demilitarized Zone (DMZ)** | A portion of the network that is separated from the internal network by a firewall and also connected to the Internet via another firewall. |
| **Firewall** | A hardware or software device that provides protection to hosts from unauthorized access over the network. |
| **Infrastructure** | The network functionality and how it is managed and maintained to support network defense, incident response, network availability, and fault analysis. Including the support of internal and external business processes and how hosts are built and deployed. |
| **Multifactor authentication** | Authentication that requires a combination of at least two of the following: something you know; something you have; or something you are. For example, the debit card from your bank is two-factor authentication: It requires something you have (the card itself) and something you know (the PIN number). Requiring someone to type in multiple passwords for authentication is only single-factor authentication, because it is merely 'something you know.' Generally, the more factors, the more secure the authentication. Thus, a system that requires an ID card (something you have), a PIN (something you know), and a fingerprint scanner (something you are) is more secure than one that requires only a username/password (single factor) or ID card and PIN. |
| **Operations** | The policies, processes, procedures, and practices related to the protection |
| **People** | The members of the organization and the policies, processes, procedures, and practices related to protecting them and the organization. |
| **Public Key Infrastructure (PKI)** | An integrated set of technologies that are required to provide Public Key encryption and digital signatures. Uses a combination of public- and private-key encryption to provide key management, data integrity, and data confidentiality. |
| **Process** | A documented series of sequential tasks used to perform a business function. |
|  |  |

### Interpreting the Graphs

### BRP ranges from 0 to 100, where a higher score implies a greater amount of potential business risk for that specific AoA. It is important to note that a score of zero is not possible here; conducting business in itself implies some level of risk. It is also important to understand that there are some aspects of running a business that have no direct mitigation strategy.

### DiDI also ranges from 0 to 100. A high score indicates an environment where a greater number of measures have been taken to deploy defense-in-depth strategies in a particular AoA. The DiDI score does not reflect overall security efficacy or even resources spent on security, rather it is a reflection of the overall strategy used to defend the environment.

### Intuitively, it may seem that a low BRP score and a high DiDI score are a good outcome, but this is not always the case. The scope of this self-assessment does not allow for all factors to be taken into consideration. Significant disparity between BRP and DiDI scores in a particular AoA suggests that further examination of this AoA is recommended. When analyzing your results it is important to consider the individual scores, both BRP and DiDI, in relation to one another. A stable environment will probably be represented by relatively equal scores across all areas. Disparities between DiDI scores are a strong indicator that overall security strategy is focused on a single mitigation technique. If the security strategy does not balance people, process and technology aspects, the environment will probably be more vulnerable to attack.