

User Guide

Updated: May 2005



Microsoft® Security Assessment Tool Version 2.0





TABLE OF CONTENTS

| | |
|--|----|
| Introduction | 3 |
| Background: Assessment Process and Scope | 3 |
| Setup | 4 |
| Installation and Registration | 4 |
| Working with Customer Profiles | 5 |
| Create New Customer Profile (BRP) | 5 |
| Manage Customer Profile | 6 |
| Working with Customer Assessments | 7 |
| Create Customer Assessment | 7 |
| Update Assessment | 8 |
| Copy or Create New Assessment (for Same Company) | 8 |
| Reports | 9 |
| Appendices | 10 |
| FAQ | 10 |
| Glossary | 12 |
| Interpreting the Graphs | 13 |



INTRODUCTION

This Microsoft® Security Assessment Tool (MSAT) is designed to help you identify and address security risks in your computing environment. The tool employs a holistic approach to measuring security strategy by covering topics that encompass people, processes, and technology. Findings are coupled with recommended mitigation efforts, including links to more information for additional guidance if needed. These resources can help you learn more about the specific tools and methods that can help increase the security of your environment.

The assessment is made up of 172 questions, broken down into three categories:

- Company Information (not identifiable): 6
- Business Risk Profile: 53
- Defense-in-Depth Assessment: 113

Based on how you answer some questions in the Business Risk Profile and the Defense-in-Depth Assessment, other questions may not appear. This is intentional and part of the methodology required to provide you with the most accurate assessment.

Background: Assessment Process and Scope

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

Beginning with a series of questions about your company's business model, the tool builds a Business Risk Profile (BRP) that measures your company's business risk according to the industry and business model you selected. A second series of questions then compiles a listing of the security measures your company has deployed over time. These security measures form layers of defense, providing greater protection against security risk and specific vulnerabilities. Each layer contributes to a combined strategy for in-depth defense. This sum is referred to as the Defense-in-Depth Index (DiDI). Finally, the BRP and DiDI are compared in order to measure risk distribution across the areas of analysis (AoA): 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 necessary.

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 it should not replace a focused assessment by trained third-party assessment teams.

SETUP

Installation and Registration

Installing the Application

To install the Microsoft Security Assessment Tool application on your local workstation or laptop (see Figure 1). Administration rights may be required.

Once you have accepted the EULA, you will be given the opportunity to enter a promo code into the text field (see Figure 2). If you don't have a promo code, skip this step by selecting **Next**. A promo code is not required to install or conduct a security assessment using the MSAT.



Figure 1
The Microsoft Security Assessment Tool End User License Agreement



Figure 2
The **Promo Code** installation screen is not required to complete an assessment.

After installation is complete, close the installation application by selecting **Finish**.



WORKING WITH CUSTOMER PROFILES

Completing Microsoft Security Assessments requires tracking customers (or multiple divisions, offices, or subsidiaries) through the BRPs, or Business Risk Profiles. Creating customer profiles may help keep assessment data for multiple customers separate and starts the assessment process by establishing the business risk of the company (see BRP in the glossary on page 12).

Create New Customer Profile (BRP)

After installation and partner profile setup, you can create a new customer profile by selecting Start from the partner profile setup screen or selecting **Create New Profile** from the left-hand navigation pane in the MSAT. Enter the unique customer name in the **Create New Profile** screen (see Figure 3) and select **OK**.

Figure 3 shows a dialog box titled "Create New Profile". It contains a text input field labeled "New profile name:" with the text "Contoso Corp." entered. Below the input field are two buttons: "OK" and "Cancel".

Figure 3
Enter the company name in the Create New Profile screen.

Complete the Business Risk Profile (see Figure 4). Typically, the input of a business decision maker (BDM), C-level officer (CXO), or technical decision maker (TDM) may be required to complete this section. Note that in the first question of the BRP, the customer name should match the name you entered in the **Create New Profile / New Profile Name** text box when you created the profile.

You will be required to completely answer all questions in the Basic Information, Infrastructure Security, Application Security, Operations Security, People Security, and Environment sections before you can begin the in-depth assessment.

Figure 4 shows the "Company Settings" screen in the Microsoft Security Assessment Tool. The left sidebar shows "Profiles" with "Create New Profile" selected, and "Contoso Corp." with "Basic Information" selected. The main area is titled "Company Settings" and "Basic Information". It contains a text input field for "Company name" with "Contoso Corp." entered, and a radio button selection for "Number of desktops and laptops in use at your company?" with "150 to 299" selected. There are "Back" and "Next >" buttons at the bottom.

Figure 4
Enter company information in the **Business Risk Profile** wizard.

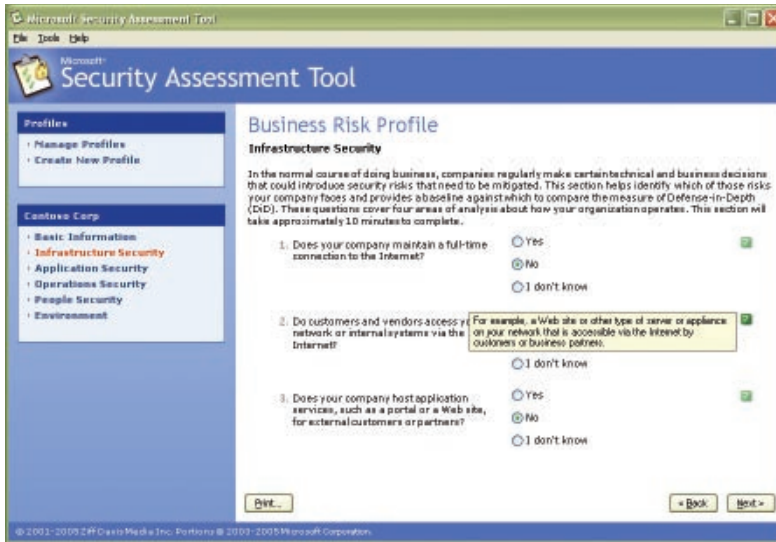




Figure 5
The MSAT offers tool tips (green question marks) to provide more information during the assessment.

TIP

Selecting the green question mark  provides more information and guidance on how to answer the question (see Figure 5).

Selecting the orange star  provides additional guidance on industry standards and best practices.

When the Business Risk Profile is complete, you will be prompted to complete a new assessment. You may either begin this phase (see Working with Customer Assessments on page 7) or select **Cancel** from the **Create New Assessment** window that appears.

Manage Customer Profile

While BRPs are not intended to be updated on a regular basis, companies may occasionally change business focus, requiring an update to the BRP.

To update a company's Business Risk Profile, select **Manage Profiles** from the left-hand navigation pane. From the companies that appear, highlight the appropriate company and select **Edit** from the buttons at the right of the profile screen (see Figure 6).

You will then be able to edit the customer's profile in the same screens used to set up a new profile. The data is saved as you make changes.

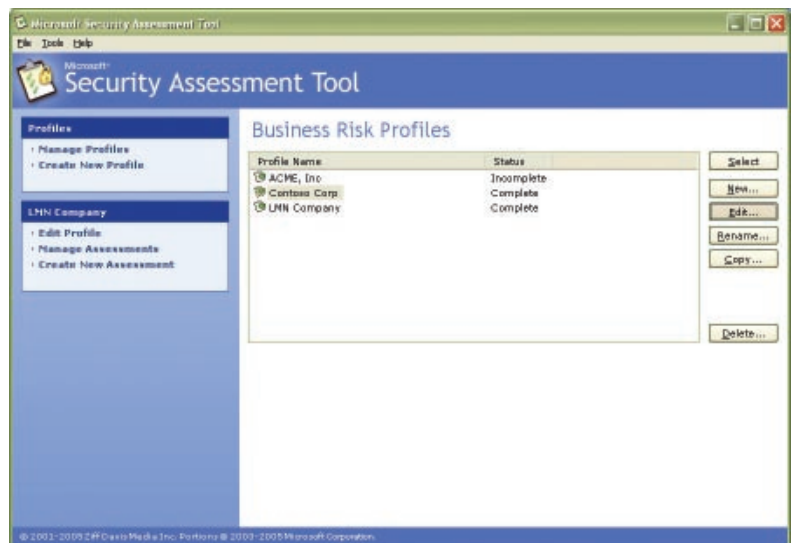


Figure 6
Manage multiple customer profiles using the MSAT.



WORKING WITH CUSTOMER ASSESSMENTS

Create Customer Assessment

After you complete a Business Risk Profile, a **Create New Assessment** window will appear so you can create a new assessment. You can create a new assessment when completing a Business Risk Profile or at any other time.

“Microsoft Security Assessment” will appear as the default and only option in the **Product** field. Enter the unique customer assessment name in the **Assessment Name** field. In the example at right, the assessment is labeled with a date, a description, and the initials of the individual completing the assessment. You can name the assessment using any standard alphanumeric convention; however, consider using a standard that will allow you to quickly identify and trace assessments within your organization (see Figure 7).

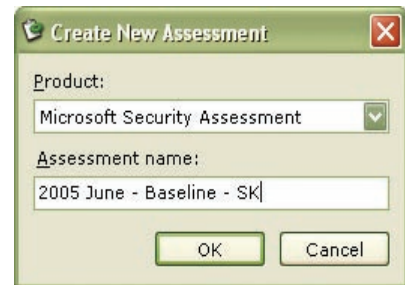


Figure 7
Use a custom convention to name your customers' assessments.

Once the assessment loads, begin completing each section.

Note that, based on how you answer particular questions during the Defense-in-Depth portion of the assessment, some answers may not be available for you to complete and will appear dimmed (see Figure 8). This is intentional and part of the methodology required to provide you with the most accurate assessment.

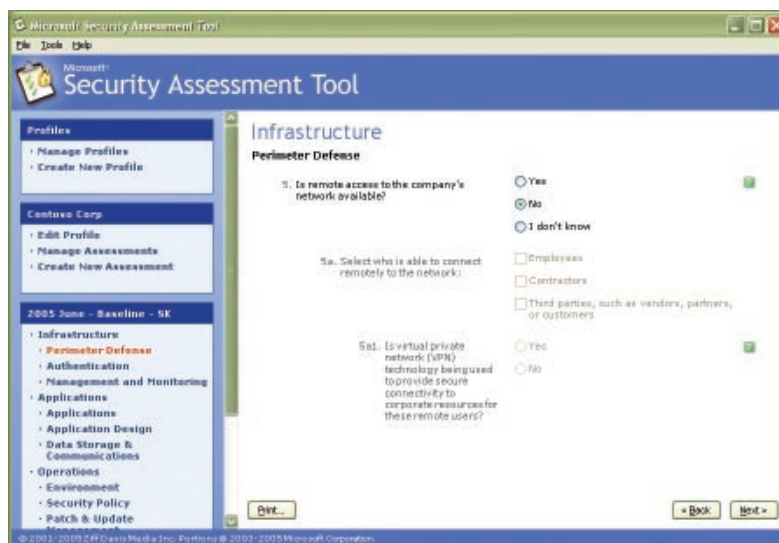


Figure 8
Not all questions will be available, depending on your answers to previous questions.

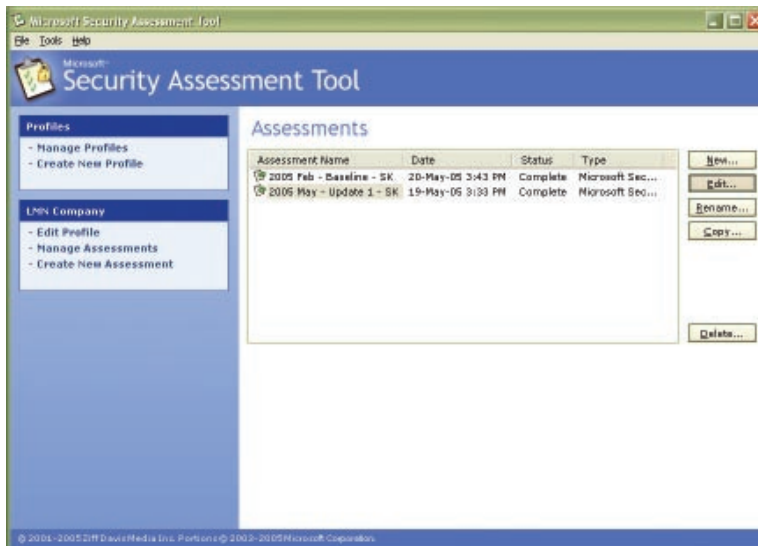


Figure 9
Use the **Manage Assessments** screen to edit or update any customer assessment.

Update Assessment

To update an assessment, you must first be in the **Manage Assessments** section of a selected company (or profile). Once you are in that section, select the appropriate assessment from the **Assessment Name** category and select **Edit** from the buttons at the right of the profile screen (see Figure 9).

Copy or Create New Assessment (for Same Company)

To copy a new assessment for the same company, in the **Manage Assessments** section of a selected company (or profile), select the appropriate assessment from the **Assessment Name** category and select **Copy** from the buttons at the right of the profile screen. To create a new assessment, choose **New** from the buttons at the right of the profile screen.

You will then be able to edit the customer's profile in the same screens used to set up a new profile. The data is saved as you make changes.

The **Manage Assessments** view allows you to create, edit, rename, or copy assessments for a specific customer. Note that in Figure 9 above, the name of the company profile is referenced in the second box appearing in the left-hand navigation pane.

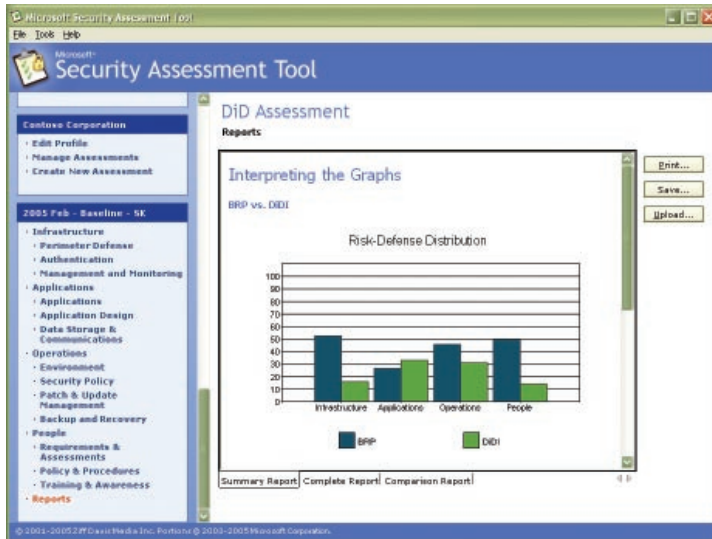


Figure 10
Three report types are available once the assessment is complete.

Summary Report The Summary Report (shown in Figure 10 above) provides a quick view of the Risk-Defense Distribution (see the glossary on page 12).

Complete Report The Complete Report provides a complete view of the findings from the Microsoft Security Assessment, including an Executive Summary, Assessment in Detail, Prescriptive Guidance, and Prioritized Action List.

Comparison Report The Comparison Report allows a company to compare any one assessment against another assessment for the same company. It also provides an industry comparison (see Figure 11) against other companies of differing sizes within various industry groups. Partners and customers are required to upload their data (BRP and DiDI) to Microsoft via the MSAT prior to viewing, printing, or saving any of the comparison reports.

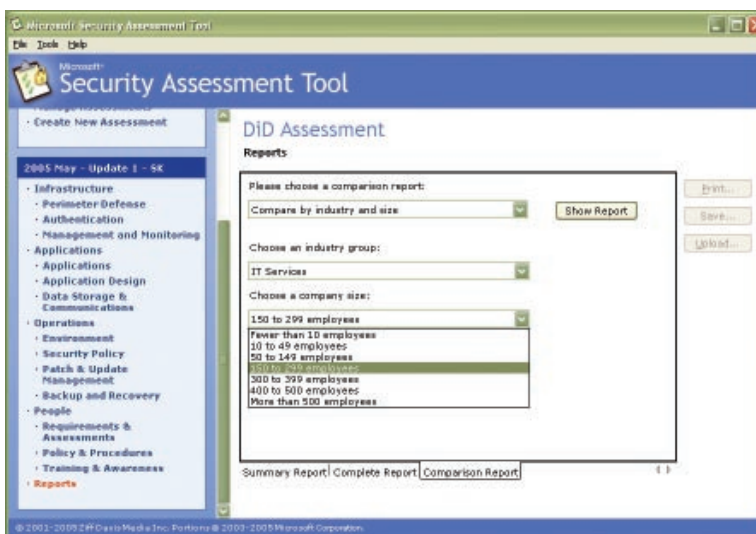


Figure 11
The MSAT Comparison Report allows for an industry comparison.

Reports

Once you have completed all sections, you will be able to view three reports: Summary Report, Complete Report, and Comparison Report (see Figure 10). The Comparison Report option allows you to compare any one customer's assessment against another assessment for the same customer or against other companies within a particular industry and company size.

All reports and data can be printed from the assessment tool, saved locally as an MHTML document, and formatted for presentation in Microsoft Word or a similar application.



APPENDICES

FAQ

1. What is a Microsoft Security Assessment?

The Microsoft Security Assessment is designed to help Microsoft Certified Partners gain a better understanding of their customers' security gaps and risks. A Microsoft Security Assessment—using the Microsoft Security Assessment Tool (MSAT)—is an interactive session that includes an on-site questionnaire. Sessions are facilitated by partners and can last from one to two hours.

The assessment provides a customer with a broad overview of its company and IT organization and results in a clearly defined map to becoming more secure through prioritized activities, solutions, and prescriptive guidance. The MSAT is a repeatable, scalable, and predictable tool focused on core solutions and services that leverages partner skill sets and demonstrates value to customers.

Participating partners are provided with the Microsoft Security Assessment Tool. This tool enables the partner to analyze the customer's corporate and IT organization. After doing so, the partner will deliver a complimentary report with findings and recommendations specific to business issues that were discussed in the session. This document is designed to help the customer understand a baseline of security and prioritize steps to mitigate identified risks through Microsoft products and partner solutions.

2. What are the goals of the Microsoft Security Assessment?

The MSAT is focused on providing partners with a common framework with which to discuss security concerns with customers. Microsoft developed the MSAT to help partners gain a holistic understanding of their customers' security risks and gaps, develop a road map to becoming more secure, and develop recurring opportunities to offer relevant Microsoft products and partner solutions.

3. Who was involved in building this tool?

The MSAT development team included Microsoft, Symantec, and Ziff Davis.

4. Is the MSAT just another effort to sell only Microsoft products?

No. The goal of the MSAT is to help customers understand the risks that their business is exposed to by their computing infrastructure, and the steps that they can take to help mitigate risk.

5. What type of guidance does the MSAT provide?

MSAT reporting provides prescriptive guidance based on industry and security standards. Suggested security resources include Microsoft, Symantec, CERT, Cisco, and similar companies.

6. Does the MSAT scan my customer's system?

No. The MSAT is a survey-based security questionnaire. In addition to assessing technology, the MSAT is designed to evaluate people and processes, which requires human input. The MSAT has no ability to collect information about local systems or networks.

7. What information is this tool collecting about my customer?

The MSAT only collects generic, nonidentifiable information: company size and industry, along with BRP and DiDI score. This data is used to compare customers with all other participants or with other participants within the same industry. The data is also used to benchmark and compare a customer's results over time. This data, however, is not collected unless you provide the survey-based answers. You can use the tool to model your customer's environment or forecast how certain improvements would impact the customer's overall score or security posture.



8. What do Symantec and Ziff Davis know about security?

Symantec was responsible for designing the questions, answers, and scoring of the tool. Ziff Davis programmed the tool and hosts it on Securityguidance.com. Symantec is much more than the company behind Norton AntiVirus. The Symantec staff who worked on the MSAT were formerly employed by @stake and joined Symantec as part of an acquisition. Well regarded as one of the premier security consulting firms in the world, @stake brought extensive experience and understanding of midmarket companies to the MSAT.

9. Why should I trust this tool?

While not a replacement for a trained consultant who knows your customer's business, the MSAT was designed to help guide companies down the road to security awareness. The questions that make up the survey portion of the tool and the associated answers are derived from commonly accepted best practices in security, both general and specific. The questions and the recommendations that the tool offers are based on standards such as ISO 17799 and NIST-800.x, as well as recommendations and prescriptive guidance from both Microsoft and external security sources.

10. What does it mean to have a high Business Risk Profile?

In the normal course of doing business, customers will regularly make technical and business decisions that may introduce security risks that need to be mitigated. The Business Risk Profile (BRP) helps identify those risks and provides a baseline against which to compare the Defense-in-Depth score.

The BRP is a measure of how much risk is associated with the way a customer does business or interacts with other businesses or customers. It is focused primarily on technical and operational risk. Having a high BRP indicates that a customer is operating in a risk-intense environment, has significant competition, or is threatened by both direct and indirect attack through systems, tools, or processes it uses.

11. My customer has a lot of defenses in place to mitigate risk. Why is the BRP still high?

The BRP is not influenced by any risk mitigation techniques in use. It should be considered a measure of the risk the organization would have without protections in place. This should be used to identify key areas where the customer may be at greater risk based on the type of business that is conducted.

12. What is Microsoft going to do with the information from this assessment if data is uploaded?

The data captured during the assessment will be used to compile peer-to-peer comparison reports available as one of the report types in MSAT. The data is uploaded in an anonymous and aggregated format and is not identifiable to any individual or organization.

13. Does a partner have to assist when a customer is using the MSAT?

No. A partner does not have to be involved in using the MSAT. The tool is freely available to anyone who wishes to use it. However, it may be desirable to use a security partner to help a customer complete the assessment or review the results of the assessment. The partners associated with the Microsoft Security Assessment Program have received specific training in the use of the MSAT and the ideas of Defense-in-Depth and Risk Mitigation. These partners also have access to other programs and information directly from Microsoft that may be of great benefit to the security efforts of your company.



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 |
|--|---|
| Antivirus (AV) | Software and hardware technologies that protect the computing environment from malicious software. |
| Application | A software program that provides functionality to an end user. Requires an operating system to run. Examples include word processor, spreadsheet, and database programs. |
| 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, processes, 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 by another firewall. |
| Firewall | A hardware or software device that provides protection to hosts from unauthorized access over the network. |
| 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 has two-factor authentication: it requires something you have (the card itself) and something you know (the PIN). 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 and password (single factor) or ID card and PIN. |
| Operations | The policies, processes, procedures, and practices related to the protection and maintenance of the organization. |
| People | The members of the organization and the policies, processes, procedures, and practices related to protecting them and the organization. |
| Process | A documented series of sequential tasks used to perform a business function. |
| 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 key and private key encryption to provide key management, data integrity, and data confidentiality. |
| Risk-Defense Distribution | The Risk-Defense Distribution is an indicator of the difference between your Business Risk Profile (BRP) and your Defense-in-Depth Index (DiDI) scores. It is used to provide you with some focus around the major areas of difference between risks and the defensive measures you have implemented. 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 information security resources to more properly address the risk your business faces. |
| Security maturity | Security maturity is inclusive of controls (both physical and technical) and the technical acumen of IT resources, policies, processes, 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. |



Interpreting the Graphs

BRP vs. DiDI

- BRP ranges from 0 to 100, where a higher score implies a greater amount of potential business risk for that specific Area of Analysis (AoA). It is important to note that a score of zero is not possible here; conducting business in and of 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 like a low BRP score and a high DiDI score make for 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 likely 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, processes, and technology aspects, the environment will likely be more vulnerable to attack.

Security Maturity

- Security maturity for each AoA ranges from 0 to 100, where a higher score implies a greater level of security maturity within the organization. The concept of security maturity is holistic though, and the rating blends the scores from all areas to determine overall placement (Baseline, Standardized, and Optimized). This overall score ranges from 0 to 400. It is important to note that a score of zero or a score of 100 in any area is unlikely; most organizations utilize some levels of protection and are likely to be at least at baseline level. Few organizations have such a significant level of risk as to require them to invest heavily in security strategies and programs.
- Security maturity is inclusive of controls (both physical and technical) and technical acumen of IT resources, policies, processes, and maintainable practices. Security maturity can only be measured 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 compared to business risk.
- The stacked graph shows the cumulative maturity score based on four areas: Infrastructure, Applications, Operations, and People. The sum of the scores from these areas determines whether the ranking is Baseline, Standardized, or Optimized. To achieve the highest score, an organization needs to have a balanced approach to its security programs that encompasses a multilayered and proactive response to security. By comparing the relative size of the four analyzed areas, you can determine if your company's security controls are more mature in one area than another and plan for appropriate mitigation.