Microsoft®

Risk Assessment Service

Microsoft has developed a Risk Assessment service to be offered to selected U.S. customers. Our goal is simple: We want to help our customers manage risk in their complex enterprise environments. We have developed a unique approach that will help guide your security strategy to ensure coverage across the infrastructure, application, operations, and organizational elements of your enterprise. As security and risk management are on-going processes, the first Risk Assessment completed for a given environment will provide a baseline against which to measure future progress with subsequent assessments. As part of our commitment to our customers' security, Microsoft will incur the cost of the initial assessment.

Risk Assessment Overview

- Provides a broad and independent assessment of risk focusing on what is critical to your business
- Focuses on your critical network segments, application, and/or data
- Includes areas that often present the biggest challenges to interoperability
- Provides strategies to mitigate risk in your current environment, beyond the scope of the two week project
- At the end of the assessment, provides a roadmap of suggested activities to reduce risk over time
- After Microsoft has completed 50-100 assessments, customers receive a report of consolidated findings and lessons learned to help gauge how they compare to others

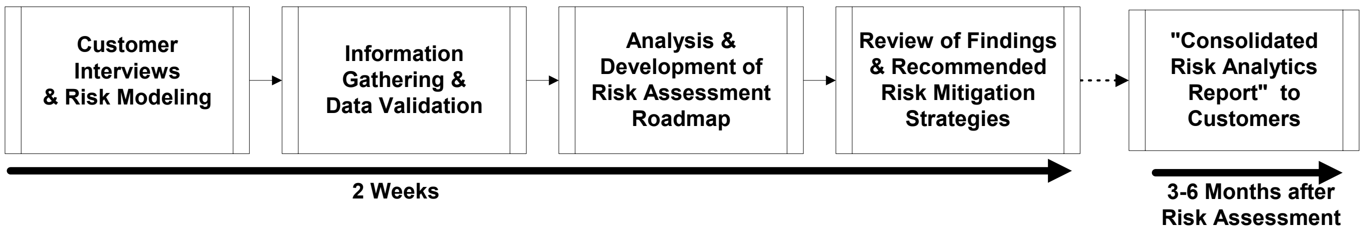
The Microsoft Risk Assessment focuses broadly on areas of information security risk across the targeted environment. Although many topics covered in the Risk Assessment may be similar to those in assessments that you already undertake, this offering is not simply a penetration test or security audit. We will work with you to identify what is critical to your business – a network segment, an application, or a specific set of data – and will evaluate the implementation of defense-in-depth strategies over a two week period, making recommendations to further mitigate risk. Instead of providing a list of specific vulnerabilities to address (as might be provided at the end of a penetration test), the Risk Assessment provides the *classes* of vulnerabilities causing risk to your environment. This allows you to begin to address issues earlier in your enterprise lifecycle. Instead of simply fixing vulnerabilities one at a time, in response to threats or attacks, you will be addressing the root causes of issues, both saving time and reducing risk.

Risk Assessment Methodology

The Detailed Methodology Ensures Quality and Repeatability

Microsoft has developed a detailed methodology on which all of the consultants performing assessments have had rigorous training. They will use a consistent approach and toolset to ensure that assessments are carried out to the same level of detail and focus regardless of the consultants performing the assessment or the customer environment selected. While the risk assessment methodology allows the customer flexibility in selection of focus areas, the process used to perform the assessment and to capture the metrics needed for risk analytics will be the same across consulting teams.

The Assessment Includes Risk Modeling, Questionnaires, Interviews, and Validation


Customer Interviews & Risk Modeling
Information Gathering & Data Validation
Analysis & Development of Risk Assessment Roadmap
Review of Findings & Recommended Risk Mitigation Strategies
"Consolidated Risk Analytics Report" to Customers
2 Weeks
3-6 Months after Risk Assessment

The assessment approach begins with a **Risk Modeling Workshop** to help the assessment team better understand your environment and perceptions of risk to the critical assets and technologies. Through this workshop, the team gathers initial information to help determine the appropriate security and risk mitigation strategies which are commensurate with acceptable business risk, defined as the project progresses.

Questionnaires are used to gather initial information about your environment, and cover a broad range of information technology and security strategy topics. They will be used as a primary means to collect information about the target environment, the use of technology, your views of what is at risk, and how it is defended. The questionnaires will also be used to gauge the level of security defenses that you have implemented, as well as the level of risk that your environment faces.

Interviews acquaint the team with the staff resources supporting the environment and ensure that accurate information was captured in the questionnaires. This gives the assessment team a head start in the analysis.

The Assessment Focuses on Pre-Defined Areas of Analysis

After the risk modeling and interviews, the assessment team will focus on validating within the four **Areas of Analysis** that provide the framework of the methodology:

Infrastructure	**Applications**	**Operations**	**People**
▪ Network Security (availability, segmentation, perimeter defense, services) ▪ Host and System Security ▪ Incident Handling ▪ Review of Network Protocols in Use	▪ Application Structure ▪ Authentication and Access Control ▪ Administration ▪ Cryptography and Encryption ▪ Database ▪ Data Integrity ▪ Logging and Auditing ▪ Web	▪ Documentation ▪ Guidelines & Policy	▪ Security Strategy ▪ Organization ▪ Incident Readiness ▪ Training and Awareness

The Deliverable: Findings, Risk Mitigation Strategies, and Risk Assessment Roadmap

After the questionnaire results have been validated and the areas of analysis assessed, the assessment team will determine the best risk management practices for your business and will recommend the necessary steps to reach them. The deliverable will be reviewed with your team on the final day of the engagement and will provide a set of recommendations for mitigating risks as well as a roadmap to develop plans and justification for funding essential security initiatives.

Risk Analytics Data

The incorporation of Risk Analytics into the Risk Assessment methodology is one of the elements that makes this assessment unique in the security-related services marketplace. Collected from the results of each engagement are standard metrics, or Risk Analytics, which will provide significant value to customers and Microsoft, as we work to effectively support secure customer environments. The consolidated analytics data from these assessments will provide trends in the use, deployment, configuration, and security of products. The risk analytics reports will provide valuable information for both you and for Microsoft development and support teams:

- **Customers:** The metrics data will help you understand how your security practices compare to your industry peers and help you support required security spending. You will see how you compare in areas such as: patch strategies and deployment timeframes, technology choices, attack surfaces, security policy, and incident response approaches. You also have an assessment that you can repeat at regular intervals to measure how effective your risk mitigation efforts have been over time.
- **Microsoft:** The metrics will help us better understand how customers are using our products in conjunction with other vendors' offerings to create business solutions. From these data, our product development teams will be able to focus on key areas of customer need, Technical Account Managers (TAMs) will be able to share new strategies to defend customer environments, and new resources will be developed to address actual customer problems.

None of the data collected for risk analytics is considered sensitive; it will all be stored in aggregate form. The resulting *Consolidated Risk Analytics Reports* could prove invaluable when communicating security posture and strategy to management, partners, and clients.

Environment Information Used in the Assessment

To assist the project team in rapidly assessing the target environment, the following types of information will be collected from customers, as available:

Infrastructure Information

- Network maps and diagrams
- Secure build documentation for hosts and devices
- Sample script files, template files, scanner or assessment results used for assessing or managing the infrastructure

Application Information

- Design documents: data flows, use cases, sequence diagrams, etc.
- Secure coding guidelines
- Application and Web server build documentation

Operations Information

- Policy, process, and procedure documents pertaining to the applications, infrastructure, or data in the assessment target
- Incident response policies and procedures
- Patch and change management technologies and processes
- Back-up and recovery technologies and processes

People and Organization Information

- Organizational structure information
- Security awareness materials
- Training information or guidelines
- Documents pertaining to security strategy

Who Will Conduct the Risk Assessment?

The Risk Assessment will be delivered by one of the select group of partner companies or by Microsoft Consulting Services (MCS). All consultants conducting these Risk Assessments have received detailed training on the methodology and the custom toolset, and are supported by a Quality Assurance Manager, who provides oversight to the entire Risk Assessment Service program. Based on the timeframe you choose for the Risk Assessment, the QA Manager will pair you with an available delivery team.

To request a Risk Assessment

Contact your Microsoft Account Executive

Microsoft®

Risk Assessment Service