

|  |  |
| --- | --- |
| Microsoft Threat Modeling Tool 2014  Getting Started Guide | |
| Microsoft Trustworthy Computing Secure Development |  |

Contents

[Overview 2](#_Toc372299034)

[Installation 2](#_Toc372299035)

[For Previous Users of Threat Modeling Tool 2](#_Toc372299036)

[System Requirements 2](#_Toc372299037)

[Download Link 2](#_Toc372299038)

[Uninstall 2](#_Toc372299039)

[Walkthrough 3](#_Toc372299040)

[Starting Threat Modeling Tool 2014 3](#_Toc372299041)

[Creating a New Threat Model 3](#_Toc372299042)

[Opening an Existing Threat Model 9](#_Toc372299043)

[Converting a Threat Model from .tms (TMT 3.1.8) Format to .tm4 (TMT 2014) Format 10](#_Toc372299044)

[Support 11](#_Toc372299045)

# Overview

The Microsoft Threat Modeling Tool 2014 (TMT) is designed to guide you and your product team through the threat modeling process. TMT functionality includes:

* An easy drawing environment.
* Automatic threat generation using the STRIDE per interaction approach.
* An option for user-defined threats to be added.

Using Microsoft Threat Modeling Tool (TMT) you can graphically identify processes and data flows that comprise an application or service.

# Installation

## For Previous Users of Threat Modeling Tool

If you have a previous version of Microsoft Threat Modeling Tool, such as TMT 3.1.8 or earlier, you should be able to run it side-by-side with Microsoft Threat Modeling Tool 2014.

## System Requirements

### Operating System Support

The table shows the operating systems supported by Microsoft Threat Modeling Tool 2014.

|  |  |
| --- | --- |
| **Operating System** | **Supported** |
| Windows Vista | No |
| Windows 7 | Yes |
| Windows 8 | Yes |
| Windows 8.1 | Yes |
| Windows 8 ARM | No |
| Windows Server 2008 R2 | Yes |
| Windows Server 2012 | Yes |
| Windows Server 2008 R2 Server Core installation Option | No |
| Windows Server 2012 Server Core installation option | No |

Table Supported Operating Systems

## Download Link

Microsoft Threat Modeling Tool 2014 and supporting documentation can be downloaded from <http://microsoft.com/security/sdl>.

## Uninstall

1. Go to **Control Panel > Programs and Features**.
2. Right-click **Microsoft Threat Modeling Tool 2014** and select **Uninstall**.

# Walkthrough

This guide will provide basic guidance on how to create a new threat model. This Getting Started Guide covers:

1. Creating a new threat model
2. Opening an existing threat model
3. Converting a threat model from TMT 3.1.8 format to the new TMT .tm4 format

For more details about TMT, see *Microsoft Threat Modeling Tool* *2014 User Guide*, available at <http://microsoft.com/security/sdl>.

## Starting Threat Modeling Tool 2014

To start TMT, click the TMT desktop shortcut.

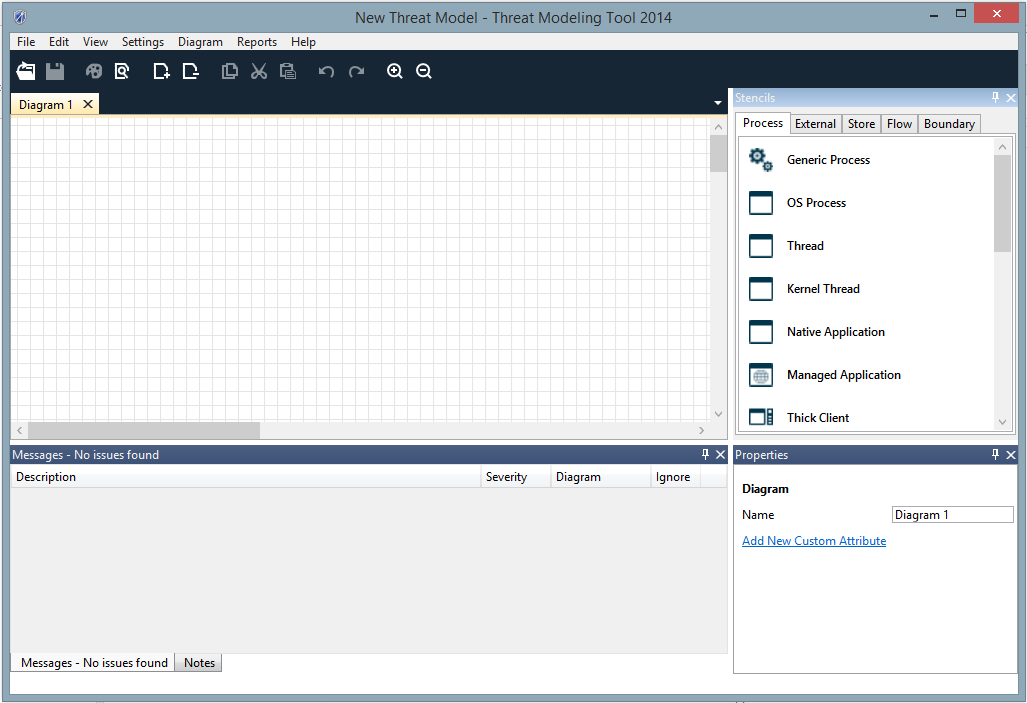
You can also start TMT from the command line. Open a command window and execute:

**C:\Program Files (x86)\Microsoft Threat Modeling Tool 2014\TMT4.exe**

## Creating a New Threat Model

This section describes the steps to create a new threat model.

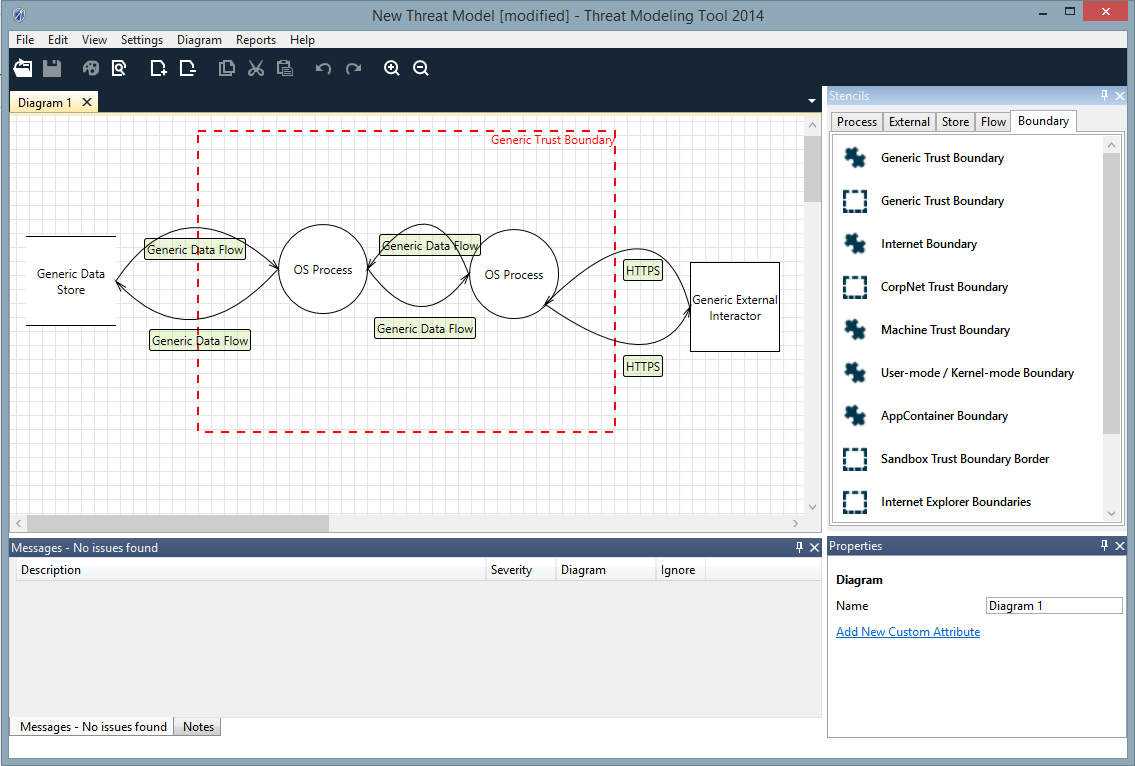
1. Start TMT and from the Home screen, click **Create a Model.** Thisbrings up the drawing surface where you will create the data flow diagram.

  
Figure Threat Modeling Tool Drawing Surface

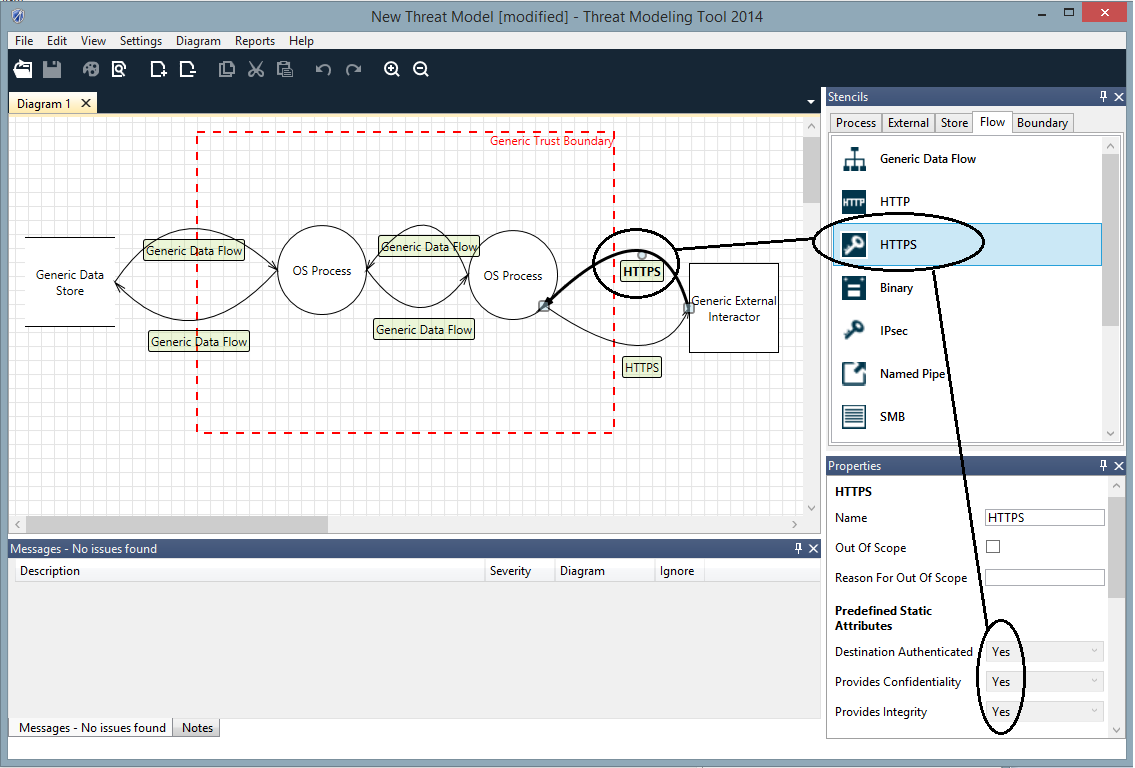
### Drawing Your Model

Draw your data flow diagram by selecting elements from the **Stencils** pane. You can select processes, external entities, data stores, data flows, and trust boundaries.

1. To select an element to draw, click on the corresponding icon in the **Stencils** pane. You can also select an element from the **Stencils** pane and drag it across the drawing surface.
2. Right-click on the drawing surface to bring up a context menu that allows you to add a generic element from each **Stencils** category.
3. To add a data flow between the two most recently selected objects, right-click the drawing surface and select **Connect** or **Bi-Directional Connect**. Alternatively, select the appropriate data flow from the **Flow** tab in the **Stencils** pane and place it on the drawing surface.

  
Figure Sample Threat Model Showing a Data Flow

1. To more fully describe the data flows in your system, specify attributes for the elements in your diagram. Right-clicking an element to convert it to another element type. If necessary, convert it from a generic element to a specific type of process, data flow, data store, external element, or trust boundary. For example, a generic data flow can be converted to HTTPS. Additionally, you can edit the properties of the element directly in the **Properties** pane.

  
Figure Identifying a Data Flow as HTTPS

### Analyzing Threats

When you have completed your data flow diagram, switch to the Analysis view by using one of the following methods:

* From the View menu, select **Analysis View**.
* Click the **Analysis View** button on the toolbar.

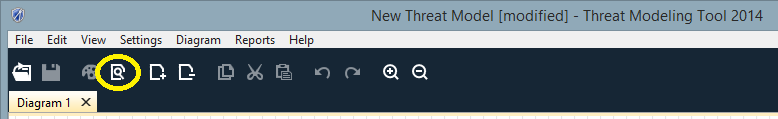


Figure Selecting Analysis View from the Toolbar

### Entering Mitigation Information

For each of your threats, enter information about how to mitigate the threat:

1. Determine if the threat requires mitigation and categorize the mitigation by selecting one of the following options from the Threat State dropdown list.
   1. Not Started
   2. Needs Investigation
   3. Not Applicable
   4. Mitigated

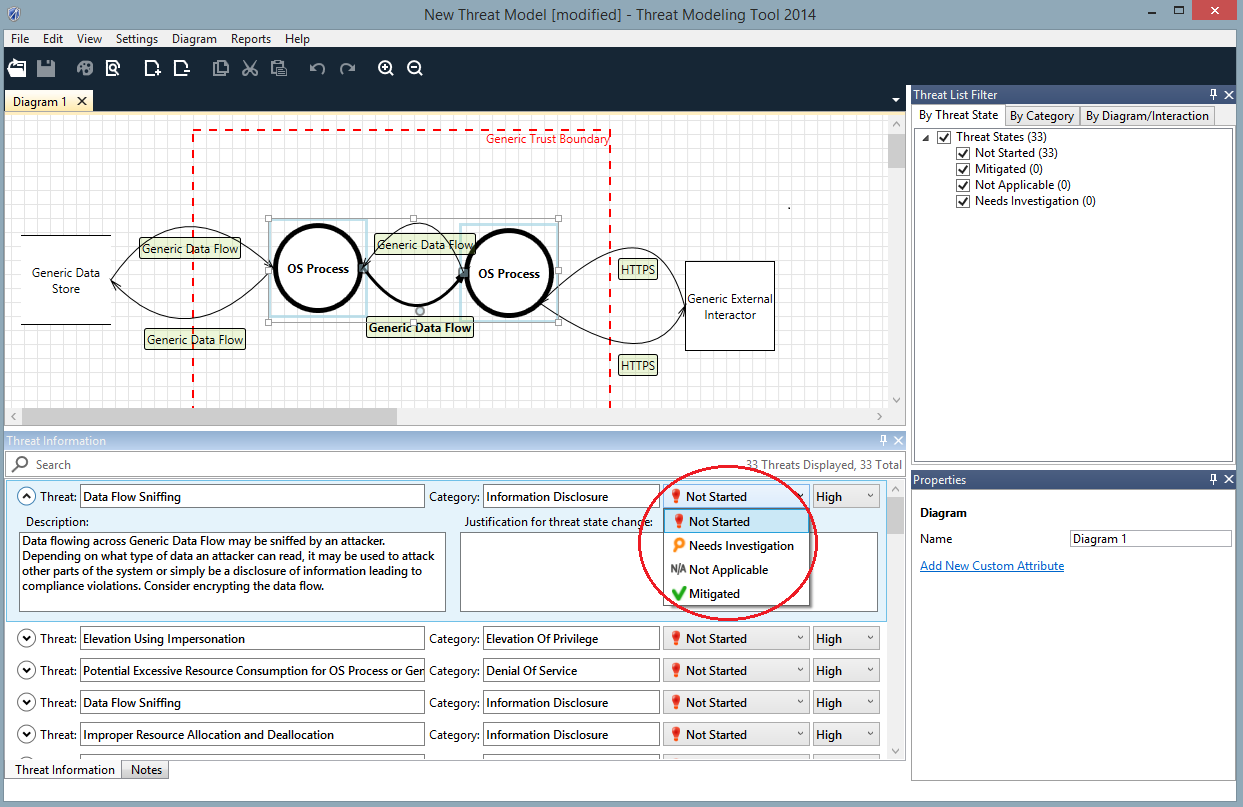


Figure Selecting Mitigation Information

1. Select one of the following threat priorities from the Threat Category dropdown list.
   1. High (default)
   2. Medium
   3. Low
2. Click the expand/collapse control on the left of each threat to view description and enter mitigation information for each threat.  
   **NOTE**: Justification is required for threats in the **Mitigated** or **Not Applicable** states.
3. Enter your mitigation information in the **Justification for threat state change** text box.

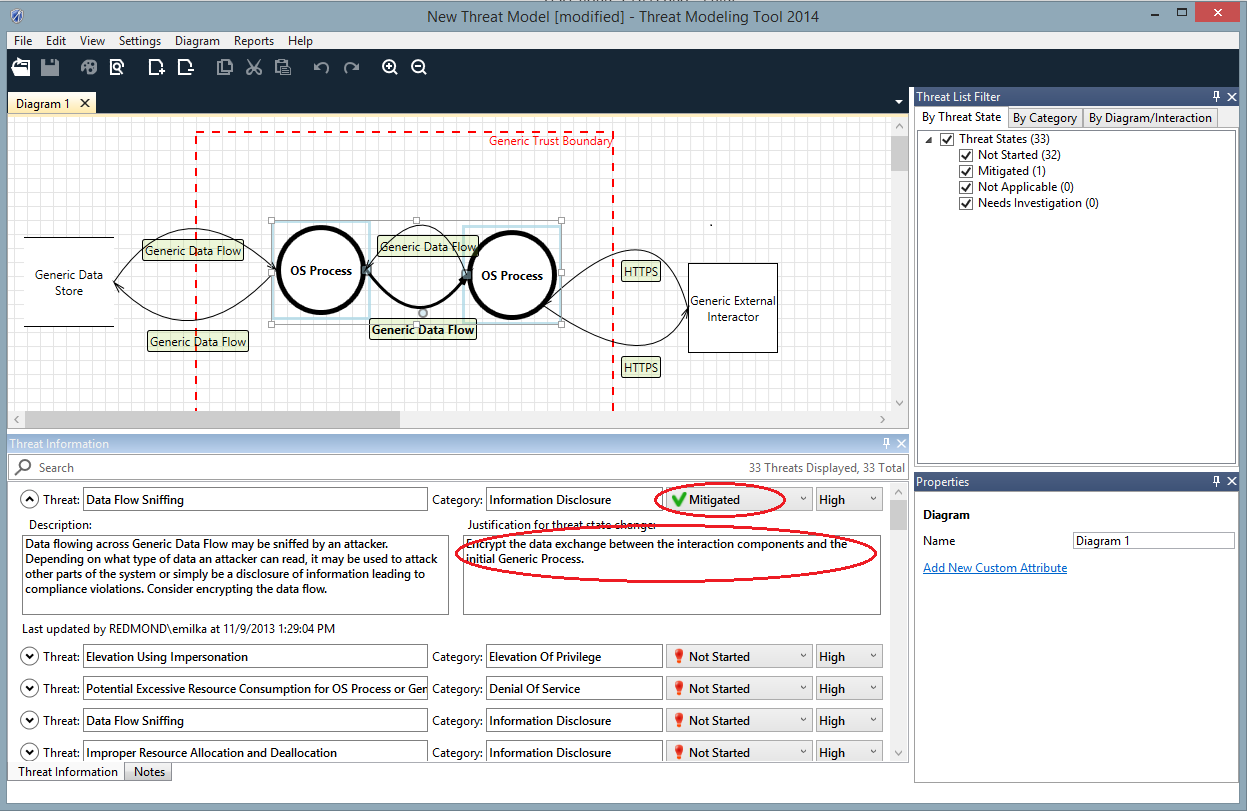


Figure Enter Justification for Threat State Change

### Finish and Create a Report

After all threats have been addressed, finish your threat model:

1. If you have not done so already, enter general information about the threat model by selecting **Model Info** from the main menu. This information includes:
   1. Review participants
   2. A brief description
   3. Answers to the security questions that address any additional risks and assumptions about the system being modeled.
2. To save the model, select **File >Save As**.
3. To create a report, select **Reports** **>Full Report**.

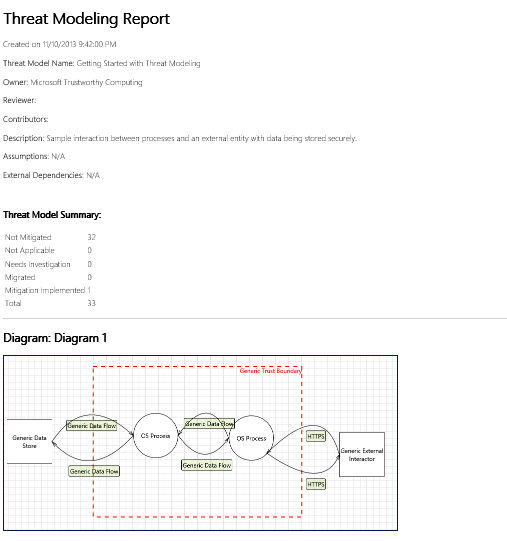


Figure Sample Threat Modeling Report

## Opening an Existing Threat Model

1. Start TMT, and from the Start screen, select the model you want under **Recently Opened Models**. If the model is not shown, select **Open A Model** and browse to the file.
2. To update the model, follow the steps described in “Creating a New Threat Model”.

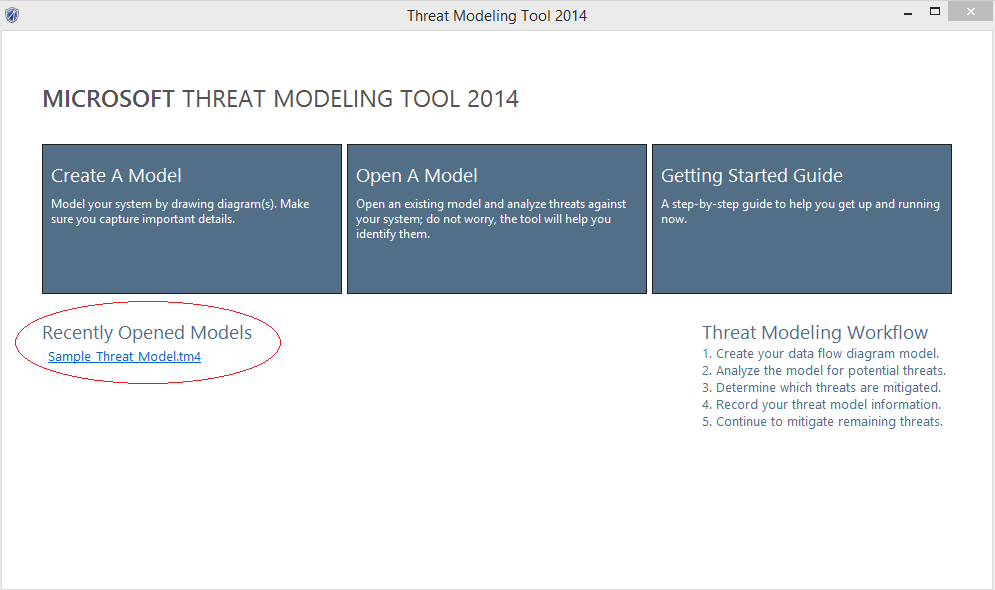


Figure Initial screen showing Recently Opened Models selected

## Converting a Threat Model from .tms (TMT 3.1.8) Format to .tm4 (TMT 2014) Format

**IMPORTANT: Threat models created with TMT 3.1.8 can only be converted if you have Visio 2007 or later installed on your machine!**

To convert a TMT 3.1.8 model (.tms file) by using the TMT GUI:

1. Start TMT, and from the Home screen select **Open A Model.**
2. In the file type combo box select **TMS(v3) files (\*.tms).**
3. Browse to a .**tms** file and click **Open.**
4. The tool will prompt you to convert the file. Click **Yes.**
5. Your model will be converted and opened immediately in the same instance of TMT.

To convert one or more TMT 3.1.8 models (.tms files) by using the stand-alone TMT converter tool:

1. Open a command window and change the path to:

**C:\Program Files (x86)\Microsoft Threat Modeling Tool 2014**

1. Enter: **TMTConvert.exe /o <full path to .tms file to be converted>**
2. To convert multiple .tms files located in same directory, enter:

**TMTConvert.exe /r <full path to .tms files to be converted>**

**Note**: Your converted diagram may not look exactly the same as the original diagram, but all the elements should be present and connected correctly. Automatic threat generation is disabled for converted threat models. However, you can enable automatic threat generation through the **Settings** menu.

Note that the threats are listed as **Migrated Categories** instead of **By Category** or **By Interaction** in Analysis view.

# Support

For support, please visit the following links:

* [Microsoft Security Development Lifecycle](http://www.microsoft.com/security/sdl/default.aspx)
* [Microsoft Trustworthy Computing Blog](http://blogs.technet.com/b/trustworthycomputing)
* [MSDN Forums for SDL](http://social.msdn.microsoft.com/Forums/en-US/home?forum=sdlprocess)

Copyright © 2014 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.