Center for Internet Security®

CIS Microsoft Office PowerPoint 2013

v1.0.1 - 11-30-2016

Table of Contents

Overview

This document, Security Configuration Benchmark for Microsoft PowerPoint 2013, provides prescriptive guidance for establishing a secure configuration posture for Microsoft PowerPoint 2013 running on Windows 7. This guide was tested against Microsoft Office 2013. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft PowerPoint 2013 on a Microsoft Windows platform.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://community.cisecurity.org.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - Be practical and prudent;
  - Provide a clear security benefit; and
  - Not inhibit the utility of the technology beyond acceptable means.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Editor
Jordan Rakoske
Edward Oechsner

Recommendations

1 User Configuration

1.1 Collaboration Settings

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.1.1 Co-Authoring

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.2 Customizable Error Messages

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.3 Disable Items in User Interface

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.3.1 Custom

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.3.2 Predefined

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.4 File Tab

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.4.1 Check Accessibility

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.5 Miscellaneous

This section contains Miscellaneous settings.

1.5.1 Server Settings

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.5.2 (L1) Ensure 'Disable Slide Update' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether users can link slides in a presentation with their counterparts in a PowerPoint Slide Library.

The recommended state for this setting is: `Enabled`.

Rationale:

PowerPoint users can share and reuse slide content by storing individual slide files in a centrally located Slide Library on a server running Office SharePoint Server. Using the Slide Update feature, users can associate a slide in a presentation on a user's computer with the original slide that resides in the Slide Library on the server.

By default, each time users open a presentation that contains a shared slide, PowerPoint notifies them if the slide has been updated and provides them with the opportunity to ignore the update, append a new slide to the outdated slide, or replace the outdated slide with the updated one. In some situations, updating a slide in a presentation from an external source like a Slide Library can cause important information to be lost. An attacker could modify the data in the slide library, affecting the integrity of all slide presentations that depend upon that library.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\slide
libraries\disableslideupdate
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint
2013\Miscellaneous\Disable Slide Update
```

Impact:

Enabling this setting prevents PowerPoint from checking Slide Libraries for slide updates. Users who work with slides associated with Slide Libraries will have to use some other mechanism to update slides in their presentations. Users who do not work with Slide Libraries will not be affected by this setting.

Default Value:

Not Configured

1.6 PowerPoint Options

1.6.1 Advanced

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.6.1.1 Web Options...

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.6.1.1.1 General

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.6.2 Customize Ribbon

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.6.3 General

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.6.4 Proofing

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.6.4.1 AutoFormat as you type

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.6.5 Save

This section contains Save settings.

*1.6.5.1 (L1) Ensure 'Default file format' is set to Enabled (PowerPoint Presentation (*pptx)) (Scored)*

Profile Applicability:

- Level 1

Description:

This policy setting governs the default format for new presentation files that users create.

The recommended state for this setting is: `Enabled. (PowerPoint Presentation (*pptx))`

Rationale:

By default, when users create new PowerPoint files, PowerPoint saves them in the new *.pptx file format. Users can change this functionality by clicking the Office button, clicking PowerPoint Options, and then selecting a file format from the Default file format list.

Disabling this setting allows users to choose from any of the available default file formats. If a new PowerPoint file is created in an earlier format, some users may not be unable to open or use the file, or they may choose a format that is less secure than the PowerPoint format.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\options\defaultfor
mat
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Save\Default file format
```

Impact:

Enabling this setting does not prevent users from choosing a different file format for a new PowerPoint file, and therefore, it is unlikely to affect usability for most users.

Default Value:

Not Configured

1.6.6 Security

This sections contains settings for Security Options.

1.6.6.1 Cryptography

This section is intentionally blank and exists to ensure the structure of PowerPoint benchmarks is consistent.

1.6.6.2 Trust Center

This section contains settings for Trust Center.

1.6.6.2.1 File Block Settings

This section contains File Block Settings.

1.6.6.2.1.1 (L1) Ensure 'Default File Block Behavior' to Enabled (Blocked files are not opened) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine if users can open, view, or edit Word files.

The recommended state for this setting is: `Enabled. (Blocked files are not opened)`

Rationale:

By default, users can open, view, or edit a large number of file types in PowerPoint. Some file types are safer than others, as some could allow malicious code to become active on user computers or the network. For this reason, disabling or not configuring this setting could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\fileblock
\openinprotectedview
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\File Block Settings\Set Default File Block Behavior
```

Impact:

Enabling this setting prevents users from opening, viewing, or editing certain types of files in PowerPoint. Productivity in your organization could be affected if users who require access to any of these file types cannot access them.

Default Value:

Not Configured

1.6.6.2.2 Protected View

This section contains settings for Protected View options.

1.6.6.2.2.1 (L1) Ensure 'Document Behavior if File Validation Fails' is set to Enabled (Open in Protected View (Unchecked)) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls how Office handles documents when they fail file validation.

The recommended state for this setting is: `Enabled`. (`Open in Protected View (Unchecked))`

Rationale:

Disabling or not configuring this setting allows users to open and edit files that have failed file validation outside of Protected View. As a result, malicious code or users could become active on user computers or the network. For example, a malicious user may purposely put invalid data in a file. The invalid data could force the program to fail or execute its code in an unexpected manner, giving the malicious user control of the application.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\filevalid
ation\disableeditfrompv
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\filevalid
ation\openinprotectedview
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\Protected View\Set Document Behavior if File Validation
Fails
```

Impact:

By default, users can only open files in Protected View after the files fail validation to help prevent malicious code from running on user computers or the network. In this way, the application is protected from attacks attempting to induce unexpected execution paths. You can block files from opening at all, but this also prevents users from accessing any data in the file.

Using this setting allows the application to open files, and thus users to view valid data and detect invalid data that is visible. However, users cannot correct invalid data in the file. To do so, users must open such files on another isolated computer where this setting is set to a lower security level.

Default Value:

Not Configured

1.6.6.2.2.2 (L1) Ensure 'Do not open from the Internet zone in Protected View' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine if files downloaded from the Internet zone open in Protected View.

The recommended state for this setting is: `Disabled`.

Rationale:

Enabling this setting allows files that users download from the Internet zone open outside of Protected View. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\protected view\disableinternetfilesinpv
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to Disabled.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint Options\Security\Trust Center\Protected View\Do not open files from the Internet zone in Protected View
```

Impact:

When files open in Protected View, some functionality will be unavailable and productivity in your organization could be affected. When this is undesirable, users will have to add sites to their trusted sites list in Internet Explorer, thus allowing the files to be opened in normal view with all functionality available.

Default Value:

Not Configured

1.6.6.2.2.3 (L1) Ensure 'Turn off Protected View for attachments opened from Outlook' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine if PowerPoint files in Outlook attachments open in Protected View.

The recommended state for this setting is: `Disabled`.

Rationale:

Enabling this setting allows Outlook attachments to open outside of Protected View. Email is a common way to spread files containing malicious code. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\protected view\disableattachmentsinpv
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint Options\Security\Trust Center\Protected View\Turn off Protected View for attachments opened from Outlook
```

Impact:

Opening Office files, such as the Office versions of Word, Excel, PowerPoint, and OneNote, is a common action. Users are unlikely to notice much difference when opening and viewing files in Protected View. Users who want to modify these kinds of files must save them to a safe location and then open them.

When Office application files open in Protected View, some functionality is unavailable. The process of dragging the file to a new location and then opening it takes more time than

simply double-clicking the file to open it, modifying it, and then saving it to the same location. For these reasons, administrators may receive some complaints from users potentially confused about how to modify files originally only available to them in Protected View.

Default Value:

Not Configured

1.6.6.2.2.4 (L1) Ensure 'Do not open files in unsafe locations in Protected View' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting lets you determine if files located in unsafe locations will open in Protected View. If you have not specified unsafe locations, only the "Downloaded Program Files" and "Temporary Internet Files" folders are considered unsafe locations.

The recommended state for this setting is: `Disabled`.

Rationale:

Enabling this setting allows users to open files located in unsafe locations that do not require Protected View. As a result, malicious code could become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\protected view\disableunsafelocationsinpv
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint Options\Security\Trust Center\Protected View\Do not open files in unsafe locations in Protected View
```

Impact:

The Downloaded Program Files folder and the Temporary Internet Files folder are considered unsafe locations. You may specify additional unsafe locations.

Some functionality is not available when files are opened in Protected View. In such cases, users must move the files from unsafe locations to save locations in order to access them with full functionality

Default Value:

Not Configured

1.6.6.2.3 Trusted Locations

This section contains settings for Trusted Locations.

1.6.6.2.3.1 (L1) Ensure 'Allow Trusted Locations on The Network' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether trusted locations on the network can be used.

The recommended state for this setting is: `Disabled`.

Rationale:

By default, files located in trusted locations and specified in the Trust Center are assumed to be safe. Content, code, and add-ins are allowed to load from trusted locations with minimal security and without prompting the user for permission.

By default, users can specify trusted locations on network shares or in other remote locations that are not under their direct control by selecting the Allow Trusted Locations on my network (not recommended) check box in the Trusted Locations section of the Trust Center. If a dangerous file is opened from a trusted location, it will not be subject to typical security measures and could affect users' computers or data.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\trusted
locations\allownetworklocations
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\Trusted Locations\Allow Trusted Locations on the network
```

Impact:

Disabling this setting will cause disruption for users who add network locations to the Trusted Locations list. However, this practice is discouraged (as the Allow Trusted Locations on my network (not recommended) check box itself states), so in practice it should be possible to disable this setting in most situations without causing significant usability issues for most users.

Default Value:

Not Configured

1.6.6.2.3.2 (L1) Ensure 'Disable all trusted locations' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows administrators to disable all trusted locations in the specified applications. Trusted locations specified in the Trust Center are used to define file locations that are assumed to be safe. Content, code, and add-ins are allowed to load from trusted locations with a minimal amount of security, without prompting the users for permission. If a dangerous file is opened from a trusted location, it will not be subject to standard security measures and could harm users' computers or data.

The recommended state for this setting is: `Enabled`.

Rationale:

Trusted locations specified in the Trust Center are used to define file locations that are assumed to be safe. Content, code, and add-ins are allowed to load from trusted locations with a minimal amount of security, without prompting the users for permission. If a dangerous file is opened from a trusted location, it will not be subject to standard security measures and could harm users' computers or data.

By default, files located in trusted locations (those specified in the Trust Center) are assumed to be safe.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\trusted
locations\alllocationsdisabled
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\Trusted Locations\Disable all trusted locations
```

Impact:

If there are business-critical reasons to access some files in a more trusted environment, disabling trusted locations could cause usability problems.

Default Value:

Not Configured

1.6.6.2.4 (L1) Ensure 'Disable Trust Bar Notification for Unsigned Application Add-ins and Block Them' is set to Enable (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether the specified Office application notifies users when unsigned application add-ins are loaded or silently disable such add-ins without notification. This policy setting only applies if you enable the "Require that application add-ins are signed by Trusted Publisher" policy setting, which prevents users from changing this policy setting.

The recommended state for this setting is: `Enabled`.

Rationale:

By default, if an application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\notbpromp
tunsignedaddin
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\Disable Trust Bar Notification for Unsigned Application
Add-ins and Block Them
```

Impact:

This setting only applies if the Office application is configured to require that all add-ins are signed by a trusted publisher. By default, users can configure this requirement themselves

in the Add-ins category of the Trust Center for the application. To enforce this requirement, you must enable the Require that application add-ins are signed by Trusted Publisher setting in Group Policy, which prevents users from changing the setting themselves.

Default Value:

Not Configured

1.6.6.2.5 (L1) Ensure 'Trust Access to Visual Basic Project' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether automation clients such as Microsoft Visual Studio 2005 Tools for Microsoft Office (VSTO) can access the Visual Basic for Applications project system in the specified applications. VSTO projects require access to the Visual Basic for Applications project system in Excel, PowerPoint, and Word, even though the projects do not use Visual Basic for Applications. Design-time support of controls in both Visual Basic and C# projects depends on the Visual Basic for Applications project system in Word and Excel.

The recommended state for this setting is: `Disabled`.

Rationale:

VSTO projects require access to the Visual Basic for Applications project system in Excel, PowerPoint, and Word, even though the projects do not use Visual Basic for Applications. Design-time support of controls in both Visual Basic and C# projects depends on the Visual Basic for Applications project system in Word and Excel.

By default, Excel, Word, and PowerPoint do not allow automation clients to have programmatic access to VBA projects. Users can enable this by selecting the Trust access to the VBA project object model in the Macro Settings section of the Trust Center. However, doing so allows macros in any documents the user opens to access the core Visual Basic objects, methods, and properties, which represents a potential security hazard.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\accessvbo
m
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\Trust Access to Visual Basic Project
```

Impact:

Disabling this setting enforces the default configuration in Excel, Word, and PowerPoint and is therefore unlikely to cause significant usability issues for most users.

Default Value:

Not Configured

1.6.6.2.6 (L1) Ensure 'Require That Application Add-ins are Signed by Trusted Publisher' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether add-ins for this applications must be digitally signed by a trusted publisher.

The recommended state for this setting is: `Enabled`.

Rationale:

By default, Office applications do not check the digital signature on application add-ins before opening them. Disabling or not configuring this setting may allow an application to load a dangerous add-in. As a result, malicious code could become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\requiread
dinsig
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\Require That Application Add-ins are Signed by Trusted
Publisher
```

Impact:

Enabling this setting could cause disruptions for users who rely on add-ins that are not signed by trusted publishers. These users will either have to obtain signed versions of such add-ins or stop using them.

Office stores certificates for trusted publishers in the Internet Explorer trusted publisher store. Earlier versions of Office stored trusted publisher certificate information

(specifically, the certificate thumbprint) in a special Office trusted publisher store. Office still reads trusted publisher certificate information from the Office trusted publisher store, but does not write information to this store.

Therefore, if you created a list of trusted publishers in a previous version of Office and you upgrade to the Office release, your trusted publisher list will still be recognized. However, any trusted publisher certificates that you add to the list will be stored in the Internet Explorer trusted publisher store.

Default Value:

Not Configured

1.6.6.2.7 (L1) Ensure 'VBA Macro Notification Settings' is set to Enabled (Disable all Except Digitally Signed) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls how the specified applications warn users when Visual Basic for Applications (VBA) macros are present.

The recommended state for this setting is: `Enabled`.

Rationale:

By default, when users open files in PowerPoint that contain VBA macros, PowerPoint opens the files with the macros disabled, and displays the Trust Bar with a warning that macros are present and have been disabled. Users may then enable these macros by clicking Options on the Trust Bar and selecting the option to enable them.

Disabling or not configuring this setting may allow dangerous macros to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\vbawarnin
gs
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\VBA Macro Notification Settings
```

Impact:

This configuration causes documents and templates that contain unsigned macros to lose any functionality supplied by those macros. To prevent this loss of functionality, users can install the macros in a trusted location, unless the Disable all trusted locations setting is

configured to Enabled, which will block them from doing so. If your organization does not use any officially sanctioned macros, consider choosing No Warnings for all macros but disable all macros for even stronger security.

Default Value:

Not Configured

1.6.6.3 (L1) Ensure 'Make Hidden Markup Visible' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether hidden markup is visible when users open PowerPoint files in standard or HTML format.

The recommended state for this setting is: `Enabled`.

Rationale:

PowerPoint presentations that are saved in standard or HTML format can contain a flag indicating whether markup (comments or ink annotations) in the presentation should be visible when the presentation is open. By default, PowerPoint ignores this flag when opening a file, and always displays any markup present in the file. In addition, when saving a file, PowerPoint sets the flag to display markup when the presentation is next opened.

If this default configuration is changed, PowerPoint sets the flag according to the state of the Show Markup option on the Review tab of the Ribbon when it saves presentations in standard or HTML format. In addition, PowerPoint enables or disables the Show Markup option according to the way the flag is set when it opens files, which means that a presentation saved with hidden markup is opened with the markup still hidden.

If a file is saved with hidden markup, users might inadvertently distribute sensitive comments or information to others via the presentation file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\options\markupopensave
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Make Hidden Markup Visible
```

Impact:

If this setting is Enabled, hidden markup will be visible when the file is opened, and if users intend it to be hidden they will need to hide it again. (Users can permanently locate and remove undesired markup from files by using the Document Inspector feature in PowerPoint.) Enabling this setting enforces the default configuration in PowerPoint.

In most cases, markup is intended to be visible to users. Markup does not display in presentation mode in PowerPoint, even if it is visible in design mode, so it is likely that this setting will have a minimal impact on usability.

Default Value:

Not Configured

1.6.6.4 (L1) Ensure 'Scan Encrypted Macros in PowerPoint Open XML Presentations' is set to Enabled (Scan Encrypted Macros) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether encrypted macros in Open XML presentations are required to be scanned with anti-virus software before being opened.

The recommended state for this setting is: `Enabled. (Scan Encrypted Macros)`

Rationale:

When an Office Open XML presentation is rights-managed or password-protected, any macros that are embedded in the presentation are encrypted along with the rest of the workbook's contents. By default, these encrypted macros will be disabled unless they are scanned by antivirus software immediately before being loaded.

If this setting is Disabled, PowerPoint will not require encrypted macros to be scanned before loading. PowerPoint will handle them as specified by the Office System macro security settings, which can cause macro viruses to load undetected and lead to data loss or reduced application functionality.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\powerpoin
tbypassencryptedmacroscan
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Scan Encrypted Macros in PowerPoint Open XML Presentations
```

Impact:

Enabling this setting enforces the default configuration in PowerPoint, and is therefore unlikely to cause usability issues for most users.

Default Value:

Not Configured

1.6.6.5 (L1) Ensure 'Run Programs' is set to Enabled (Disable (Don't Run Any Programs)) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls the prompting and activation behavior for the "Run Programs" option for action buttons in PowerPoint.

The recommended state for this setting is: `Enabled`. `(Disable (Don't Run Any Programs))`

Rationale:

Action buttons can be used to launch external programs from PowerPoint presentations. If a malicious person adds an action button to a presentation that launches a dangerous program, it could significantly affect the security of a user's computer and data.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\runprograms
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint Options\Security\Run Programs
```

Impact:

Enabling this setting and configuring the drop-down menu to "Disable (don't run any programs)" will cause disruptions to users who wish to create or use presentations that launch external programs when action buttons are clicked. These users will have to launch any external programs manually at the appropriate times when delivering presentations.

Default Value:

Not Configured

1.6.6.6 (L1) Ensure 'Turn Off File Validation' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you turn off the file validation feature.

The recommended state for this setting is: `Disabled`.

Rationale:

The file validation feature ensures that Office Binary Documents are checked to see if they conform against the file format schema before they are opened, which may help protect against certain types of attacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\filevalid
ation\enableonload
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Turn Off File Validation
```

Impact:

If you enable this policy setting, file validation will be turned off. If you disable or do not configure this policy setting, file validation will be turned on. Office Binary Documents (97-2003) are checked to see if they conform against the file format schema before they are opened.

Default Value:

Not Configured

1.6.6.7 (L1) Ensure 'Unblock Automatic Download of Linked Images' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether PowerPoint automatically downloads links from external sources.

The recommended state for this setting is: `Disabled`.

Rationale:

When users insert images into PowerPoint presentations, they can select Link to File instead of Insert. If they do so, the image is represented by a link to a file on disk instead of being embedded in the presentation file itself.

By default, when PowerPoint opens a presentation it does not display any linked images saved on a different computer unless the presentation itself is saved in a trusted location (as configured in the Trust Center). If this configuration is changed, PowerPoint will load any images that were saved in remote locations, which presents a security risk.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\downloadi
mages
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Unblock Automatic Download of Linked Images
```

Impact:

Disabling this setting enforces the default configuration of PowerPoint, and is therefore unlikely to cause significant usability issues for most users.

Default Value:

Not Configured

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**User Configuration**		
1.1	**Collaboration Settings**		
1.1.1	**Co-Authoring**		
1.2	**Customizable Error Messages**		
1.3	**Disable Items in User Interface**		
1.3.1	**Custom**		
1.3.2	**Predefined**		
1.4	**File Tab**		
1.4.1	**Check Accessibility**		
1.5	**Miscellaneous**		
1.5.1	**Server Settings**		
1.5.2	(L1) Ensure 'Disable Slide Update' is set to Enabled (Scored)	☐	☐
1.6	**PowerPoint Options**		
1.6.1	**Advanced**		
1.6.1.1	**Web Options...**		
1.6.1.1.1	**General**		
1.6.2	**Customize Ribbon**		
1.6.3	**General**		
1.6.4	**Proofing**		
1.6.4.1	**AutoFormat as you type**		
1.6.5	**Save**		
1.6.5.1	(L1) Ensure 'Default file format' is set to Enabled (PowerPoint Presentation (*pptx)) (Scored)	☐	☐
1.6.6	**Security**		
1.6.6.1	**Cryptography**		
1.6.6.2	**Trust Center**		
1.6.6.2.1	**File Block Settings**		
1.6.6.2.1.1	(L1) Ensure 'Default File Block Behavior' to Enabled (Blocked files are not opened) (Scored)	☐	☐
1.6.6.2.2	**Protected View**		
1.6.6.2.2.1	(L1) Ensure 'Document Behavior if File Validation Fails' is set to Enabled (Open in Protected View (Unchecked)) (Scored)	☐	☐
1.6.6.2.2.2	(L1) Ensure 'Do not open from the Internet zone in Protected View' is set to Disabled (Scored)	☐	☐
1.6.6.2.2.3	(L1) Ensure 'Turn off Protected View for attachments opened from Outlook' is set to Disabled (Scored)	☐	☐
1.6.6.2.2.4	(L1) Ensure 'Do not open files in unsafe locations in Protected	☐	☐

	View' is set to Disabled (Scored)		
1.6.6.2.3	**Trusted Locations**		
1.6.6.2.3.1	(L1) Ensure 'Allow Trusted Locations on The Network' is set to Disabled (Scored)	☐	☐
1.6.6.2.3.2	(L1) Ensure 'Disable all trusted locations' is set to Enabled (Scored)	☐	☐
1.6.6.2.4	(L1) Ensure 'Disable Trust Bar Notification for Unsigned Application Add-ins and Block Them' is set to Enable (Scored)	☐	☐
1.6.6.2.5	(L1) Ensure 'Trust Access to Visual Basic Project' is set to Disabled (Scored)	☐	☐
1.6.6.2.6	(L1) Ensure 'Require That Application Add-ins are Signed by Trusted Publisher' is set to Enabled (Scored)	☐	☐
1.6.6.2.7	(L1) Ensure 'VBA Macro Notification Settings' is set to Enabled (Disable all Except Digitally Signed) (Scored)	☐	☐
1.6.6.3	(L1) Ensure 'Make Hidden Markup Visible' is set to Enabled (Scored)	☐	☐
1.6.6.4	(L1) Ensure 'Scan Encrypted Macros in PowerPoint Open XML Presentations' is set to Enabled (Scan Encrypted Macros) (Scored)	☐	☐
1.6.6.5	(L1) Ensure 'Run Programs' is set to Enabled (Disable (Don't Run Any Programs)) (Scored)	☐	☐
1.6.6.6	(L1) Ensure 'Turn Off File Validation' is set to Disabled (Scored)	☐	☐
1.6.6.7	(L1) Ensure 'Unblock Automatic Download of Linked Images' is set to Disabled (Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
8-20-15	1.0.0	Initial Release
11-30-16	1.0.1	Text and Title Cleanup